

(19)日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-73424

(P2002-73424A)

(43)公開日 平成14年3月12日(2002.3.12)

(51)IntCl. <sup>7</sup>	識別記号	F I	テマコード(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 F 5 B Q 1 7
G 0 6 K 17/00		G 0 6 K 17/00	L 5 B 0 3 5
19/00		19/00	T 5 B 0 5 8
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 S 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 D 5 K 0 6 7

審査請求 未請求 請求項の数57 O L (全 49 頁) 最終頁に続く

(21)出願番号 特願2000-262445(P2000-262445)

(22)出願日 平成12年8月31日(2000.8.31)

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 前田 茂伸

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74)代理人 100089233

弁理士 吉田 茂明 (外2名)

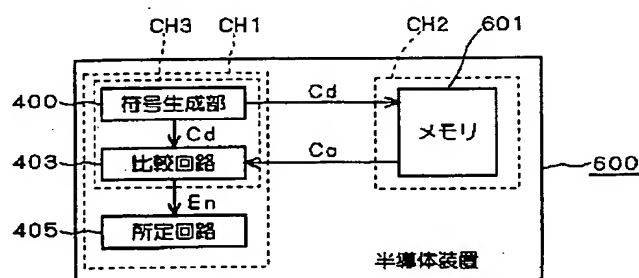
最終頁に続く

(54)【発明の名称】 半導体装置、端末装置および通信方法

## (57)【要約】

【課題】 半導体基板を取り替えてなされる半導体装置の応用機器の不正使用に対する技術的障壁を高める。

【解決手段】 符号生成部400は、半導体基板CH1(またはCH3)に固有の識別符号Cdを生成する。別の半導体基板CH2に形成されたメモリ601は、識別符号Cdを記憶符号Coとして記憶する。識別符号Cdは、半導体装置600が製品として出荷されるときに、符号生成部400からメモリ601へ書き込まれる。比較回路403は、識別符号Cdと記憶符号Coとを比較し、これら双方が互いに一致しないときには、所定回路405の一部の動作を停止する。



## 【特許請求の範囲】

【請求項 1】 少なくとも一つの半導体基板の各々に形成され、その半導体基板に固有の識別符号を生成する符号生成部と、  
前記識別符号の各々ごとに、対応する半導体基板とは別の半導体基板に形成され、対応する識別符号に一致する符号を記憶符号として記憶するメモリと、を備える半導体装置。

【請求項 2】 前記メモリが、前記記憶符号を記憶する OTPROM を備える、請求項 1 に記載の半導体装置。

【請求項 3】 前記符号生成部が、

半導体素子と、

前記半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより、前記識別符号を生成し、出力する符号化回路と、を備える、請求項 1 または請求項 2 に記載の半導体装置。

【請求項 4】 前記半導体素子が多結晶体を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する、請求項 3 に記載の半導体装置。

【請求項 5】 前記符号生成部が、前記識別符号を記憶する OTPROM を備える、請求項 1 または請求項 2 に記載の半導体装置。

【請求項 6】 前記識別符号の各々ごとに、前記識別符号と、対応する前記記憶符号とを比較し、これら双方が一致するか否かを判定し、その結果を表現する判定信号を出力する比較回路を、さらに備える、請求項 1 ないし請求項 5 のいずれかに記載の半導体装置。

【請求項 7】 前記比較回路が、比較対象とする識別符号に対応する前記半導体基板に形成されている、請求項 6 に記載の半導体装置。

【請求項 8】 前記識別符号の各々ごとに、対応する前記半導体基板に形成された鍵生成部、暗号化回路および復号化回路を、さらに備え、  
前記鍵生成部は、対応する前記半導体基板に固有である暗号化のための鍵を生成し、

前記暗号化回路は、対応する前記半導体基板に形成された前記符号生成部が生成する前記識別符号を、対応する前記鍵にもとづいて暗号化し、暗号化された形式で対応する前記メモリへ伝え、

対応する前記メモリは、前記暗号化回路が出力する暗号化された形式での前記識別符号を、暗号化された形式での前記記憶符号として記憶し、

前記復号化回路は、対応する前記メモリに記憶される暗号化された前記記憶符号を、対応する前記鍵にもとづいて復号化し、

前記比較回路は、対応する前記符号化回路が生成する前記識別符号と、対応する前記復号化回路が生成する復号化された前記記憶符号とを比較する、請求項 7 に記載の

半導体装置。

【請求項 9】 前記鍵生成部が、

別の半導体素子と、

前記別の半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより、前記鍵を生成し、出力する別の符号化回路と、を備える、請求項 8 に記載の半導体装置。

【請求項 10】 前記別の半導体素子が多結晶体を有しており、前記別の半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する、請求項 9 に記載の半導体装置。

【請求項 11】 前記鍵生成部が、前記鍵を記憶する OTPROM を備える、請求項 8 に記載の半導体装置。

【請求項 12】 前記識別符号の各々ごとに、対応する前記半導体基板に形成され、対応する前記符号化回路が生成した前記識別符号の、対応する前記メモリへの送出手、対応する前記メモリに記憶される前記記憶符号の前記比較回路への入力とを、排他的に行うスイッチ回路を、さらに備える、請求項 7 ないし請求項 11 のいずれかに記載の半導体装置。

【請求項 13】 前記識別符号の各々に対応した前記判定信号に依存して選択的に動作または非動作となる回路部分を含む所定回路を、さらに備える、請求項 6 ないし請求項 12 のいずれかに記載の半導体装置。

【請求項 14】 前記所定回路が、前記比較回路が形成されている前記少なくとも一つの半導体基板の一つに形成されている、請求項 13 に記載の半導体装置。

【請求項 15】 前記少なくとも一つの半導体基板の個数が単一である、請求項 1 ないし請求項 14 のいずれかに記載の半導体装置。

【請求項 16】 前記少なくとも一つの半導体基板の個数が 2 個であり、  
前記識別符号の各々ごとに、対応する前記符号生成部と前記メモリは、互いに前記 2 個の半導体基板の一方と他方とに形成されている、請求項 1 ないし請求項 14 のいずれかに記載の半導体装置。

【請求項 17】 半導体素子と当該半導体素子の電気的特性のばらつきに由来して値がばらつくように前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより暗号化のための鍵を生成し、出力する符号化回路とを備える鍵生成部と、  
前記鍵にもとづいて送信データを暗号化する暗号化回路と、  
前記鍵にもとづいて受信データを復号化する復号化回路と、を備える端末装置。

【請求項 18】 前記符号化回路と前記復号化回路とが本体部に組み込まれており、  
前記鍵生成部が、前記本体部に脱着自在の補助部に組み込まれている、請求項 17 に記載の端末装置。

【請求項 19】 前記補助部が IC カードである、請求項 18 に記載の端末装置。

【請求項 20】 前記半導体素子が多結晶性を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶性の結晶構造のばらつきに由来する、請求項 17 ないし請求項 19 のいずれかに記載の端末装置。

【請求項 21】 請求項 13 または請求項 14 に記載の半導体装置を備え、前記所定回路が、外部との間で信号を送信および受信する通信回路であって、前記判定信号の各々が前記識別符号の少なくとも一つと対応する前記記憶符号との間の不一致を示すときには、送信または受信の少なくとも一方を停止する端末装置。

【請求項 22】 請求項 6 ないし請求項 12 のいずれかに記載の半導体装置と、外部との間で信号を送信および受信する通信回路と、を備え、前記通信回路は、前記信号の一部として前記判定信号の各々を前記外部へ送信する端末装置。

【請求項 23】 請求項 1 ないし請求項 5 のいずれかに記載の半導体装置と、外部との間で信号を送信および受信する通信回路と、を備え、前記通信回路は、前記信号の一部として前記識別符号の各々と前記記憶符号の各々を前記外部へ送信する端末装置。

【請求項 24】 前記少なくとも一つの半導体基板の個数が単一であって、前記符号生成部の各々と前記通信回路とが本体部に組み込まれており、前記メモリの各々が前記本体部に脱着自在の補助部に組み込まれている、請求項 23 に記載の端末装置。

【請求項 25】 前記本体部には、暗号化のための第 1 鍵を生成する第 1 鍵生成部と、前記符号生成部が生成する前記識別符号を、前記第 1 鍵にもとづいて暗号化する第 1 暗号化回路と、がさらに組み込まれており、前記補助部には、暗号化のための第 2 鍵を生成する第 2 鍵生成部と、前記メモリが記憶する前記記憶符号を、前記第 2 鍵にもとづいて暗号化する第 2 暗号化回路と、がさらに組み込まれており、前記第 1 暗号化回路は、前記第 2 暗号化回路が暗号化した前記記憶符号をも、前記第 1 鍵にもとづいて暗号化し、前記通信回路は、前記第 1 暗号化回路で暗号化された形式で、前記識別符号および前記記憶符号を前記外部へ送信する、請求項 24 に記載の端末装置。

【請求項 26】 前記第 1 鍵生成部と前記第 1 暗号化回路とが、前記符号化回路が形成された前記半導体基板に

形成されている、請求項 25 に記載の端末装置。

【請求項 27】 前記第 2 鍵生成部と前記第 2 暗号化回路とが、前記メモリが形成された前記半導体基板に形成されている、請求項 25 または請求項 26 に記載の端末装置。

【請求項 28】 前記本体部が、充電可能な電池を備えており、前記補助部が、前記本体部に装着されることにより前記電池を充電する充電器である、請求項 24 ないし請求項 27 のいずれかに記載の端末装置。

【請求項 29】 前記補助部が IC カードであり、前記本体部と前記補助部の各々には、前記補助部から前記本体部への符号の伝送を無線で媒介するための通信インタフェースが、さらに組み込まれている、請求項 24 ないし請求項 27 のいずれかに記載の端末装置。

【請求項 30】 前記通信回路が、前記少なくとも一つの半導体基板の一つに前記符号生成部とともに形成されている、請求項 22 ないし請求項 29 のいずれかに記載の端末装置。

【請求項 31】 通信事業者設備を媒介した無線通信を行う通信回路と、前記通信事業者設備を媒介しない無線通信網を形成することにより無線通信を行う無線通信網回路と、を備える端末装置。

【請求項 32】 前記通信回路と前記無線通信網回路との間での通信信号の経路の接続と切断とを選択自在に実行することにより、前記無線通信網を通じての前記端末装置の使用者と他者との間の通信と、前記無線通信網を通じての前記端末装置の使用者以外の複数の他者どうしの通信の中継と、を選択自在に実現する切替回路を、さらに備える、請求項 31 に記載の端末装置。

【請求項 33】 暗号化のための鍵を生成する鍵生成部と、前記通信信号の中で前記通信回路から前記無線通信網回路へ送られる送信信号を前記鍵にもとづいて暗号化する暗号化回路と、前記通信信号の中で前記無線通信網回路から前記通信回路へ送られる受信信号を前記鍵にもとづいて復号化する復号化回路と、をさらに備え、前記鍵生成部が、前記端末装置を識別するための符号を生成する符号生成部と、前記符号生成部が生成する前記符号と、前記無線通信網回路を通じて通信相手から送られる別の符号とにもとづいて、前記使用者と前記通信相手との間で共通に使用可能な共通鍵を算出する鍵演算部と、を備える、請求項 32 に記載の端末装置。

【請求項 34】 前記符号生成部が、半導体素子と、前記半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタ

ル形式の信号へ変換することにより、前記符号を生成し、出力する符号化回路と、を備える、請求項33に記載の端末装置。

【請求項35】 前記半導体素子が多結晶体を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する、請求項34に記載の端末装置。

【請求項36】 前記符号生成部が、前記符号を記憶するOTPROMを備える、請求項33に記載の端末装置。

【請求項37】 前記通信信号の中で前記無線通信回路から前記通信回路へ送られる受信信号の経路に介挿された第1および第2ミキサを、さらに備え、前記第1ミキサは、前記通信回路が受信した受信信号を復調し、前記第2ミキサは、復調された前記受信信号を前記通信回路の周波数帯域内の周波数を有する搬送波を用いて変調する、請求項32ないし請求項36のいずれかに記載の端末装置。

【請求項38】 事業者設備と請求項2に記載の端末装置とが相互に通信を行う通信方法であって、

(a)前記端末装置が、前記判定信号の各々を前記事業者設備へ送信する工程と、  
(b)前記事業者設備が、受信した前記判定信号の各々が、前記識別符号の各々に対応する前記記憶符号との一致を示すという条件が充足されれば、前記端末装置の使用が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備える通信方法。

【請求項39】 事業者設備と請求項23に記載の端末装置とが相互に通信を行う通信方法であって、

(a)前記端末装置が、前記識別符号の各々と前記記憶符号の各々を前記事業者設備へ送信する工程と、  
(b)前記事業者設備が、受信した前記識別符号の各々に対応する前記記憶符号と比較し、一致するか否かを判定する工程と、  
(c)前記事業者設備が、前記工程(b)において前記識別符号の各々に対応する前記記憶符号に一致すると判定したという条件が充足されれば、前記端末装置の使用が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備える通信方法。

【請求項40】 (e)前記事業者設備が、受信した前記識別符号の各々と前記記憶符号の各々を記録する工程を、さらに備える、請求項39に記載の通信方法。

【請求項41】 前記工程(c)において、前記事業者設備は、前記認証を行わない場合には、受信した前記識別符号の各々と前記記憶符号の各々を記録する、請求項39に記載の通信方法。

【請求項42】 (a)事業者設備が、請求項24に記載

の端末装置の前記識別符号を得て、第1登録符号として記憶する工程と、

(b)前記事業者設備が、前記端末装置の前記記憶符号を得て、第2登録符号として記憶する工程と、

(c)前記工程(a)および(b)の後に、前記事業者設備と前記端末装置とが相互に通信を行う通信工程と、を備え、当該通信工程(c)は、

(c-1)前記補助部が前記本体部に装着されていないときに実行される第1通信工程と、

10 (c-2)前記補助部が前記本体部に装着されているときに実行される第2通信工程と、を備え、

前記第1通信工程(c-1)は、

(c-1-1)前記端末装置が、前記識別符号を前記事業者設備へ送信する工程と、

(c-1-2)前記事業者設備が、受信した前記識別符号と前記第1登録符号とを比較し、これら双方が一致するか否かを判定する工程と、

(c-1-3)前記事業者設備が、前記工程(c-1-2)で前記双方が一致すると判定したという条件が充足されれば、前記

20 端末装置の使用が正当使用者であるとの認証を行い、

前記条件が充足されなければ、前記認証を行わない認証工程と、を備え、

前記第2通信工程(c-2)は、

(c-2-1)前記端末装置が、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、

(c-2-2)前記事業者設備が、受信した前記識別符号と前記第1登録符号とを比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号と前記第2登録符号とを比較し、これら双方が一致するか否かを判定する工程と、

30 (c-2-3)前記事業者設備が、前記工程(c-2-2)の2つの判定のいずれにおいても一致するとの判定が得られたという条件が充足されれば、前記端末装置の使用が正当使用者であるとの高位の認証を行い、前記条件が充足されなければ、前記高位の認証を行わない高位認証工程と、を備える通信方法。

【請求項43】 前記工程(b)では、前記補助部が前記本体部に装着された状態で前記事業者設備と前記端末装置とが通信を行うことにより、事業者設備が、前記端末装置の前記記憶符号を得る、請求項42に記載の通信方法。

【請求項44】 前記工程(c)が、

(c-3)前記補助部が前記本体部に装着されているときに実行され、前記第2登録符号の変更を行う変更工程を、さらに備え、

前記変更工程(c-3)は、

(c-3-1)前記端末装置が、前記変更の意志を表現する要求信号とともに、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、

50 (c-3-2)前記事業者設備が、受信した前記識別符号と前

記第1登録符号とを比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号と前記第2登録符号とを比較し、これら双方が一致するか否かを判定する工程と、

(c-3-3)前記事業者設備が、前記工程(c-3-2)の2つの判定のいずれにおいても一致するとの判定結果を得たときに限って、前記変更を許可する工程と、

(c-3-4)前記工程(c-3-3)の後に、前記端末装置の前記補助部を交換し、交換後の補助部を前記本体部へ装着する工程と、

(c-3-5)前記端末装置が、前記工程(c-3-4)の後に、前記識別符号と交換後の前記補助部にもとづく変更後の前記記憶符号とを前記事業者設備へ送信する工程と、

(c-3-6)前記事業者設備が、前記工程(c-3-3)で前記変更を許可した場合に限って、受信した変更後の前記記憶符号で前記第2登録符号を更新する工程と、を備える、請求項42または請求項43に記載の通信方法。

【請求項45】 (a)事業者設備が、請求項25に記載の端末装置の前記識別符号および前記第1鍵を得て、それぞれ第1登録符号および登録鍵として記憶する工程と、

(b)前記事業者設備が、前記端末装置の前記第2鍵で暗号化された前記記憶符号を得て、第2登録符号として記憶する工程と、

(c)前記工程(a)および(b)の後に、前記事業者設備と前記端末装置とが相互に通信を行う通信工程と、を備え、当該通信工程(c)は、

(c-1)前記補助部が前記本体部に装着されていないときに実行される第1通信工程と、

(c-2)前記補助部が前記本体部に装着されているときに実行される第2通信工程と、を備え、

前記第1通信工程(c-1)は、

(c-1-1)前記端末装置が、前記第1暗号化回路で暗号化された形式で、前記識別符号を前記事業者設備へ送信する工程と、

(c-1-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第1登録符号と比較し、これら双方が一致するか否かを判定する工程と、

(c-1-3)前記事業者設備が、前記工程(c-1-2)で前記双方が一致すると判定したという条件が充足されれば、前記端末装置の使用が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備え、

前記第2通信工程(c-2)は、

(c-2-1)前記端末装置が、前記第1暗号化回路で暗号化された形式で、前記識別符号および記憶符号を前記事業者設備へ送信する工程と、

(c-2-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第1登録符

号と比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号を前記登録鍵にもとづいて復号化した上で、前記第2登録符号と比較し、これら双方が一致するか否かを判定する工程と、

(c-2-3)前記事業者設備が、前記工程(c-2-2)の2つの判定のいずれにおいても一致するとの判定が得られたという条件が充足されれば、前記端末装置の使用が正当使用者であるとの高位の認証を行い、前記条件が充足されなければ、前記高位の認証を行わない高位認証工程と、を備える通信方法。

【請求項46】 前記工程(b)では、前記補助部が前記本体部に装着された状態で前記事業者設備と前記端末装置とが通信を行うことにより、事業者設備が、前記端末装置の前記第2鍵で暗号化された前記記憶符号を得る、請求項45に記載の通信方法。

【請求項47】 前記工程(c)が、

(c-3)前記補助部が前記本体部に装着されているときに実行され、前記第2登録符号の変更を行う変更工程を、さらに備え、

前記変更工程(c-3)は、

(c-3-1)前記端末装置が、前記変更の意志を表現する要求信号とともに、前記第1暗号化回路で暗号化された形式で、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、

(c-3-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第1登録符号と比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号を前記登録鍵にもとづいて復号化した上で、前記第2登録符号と比較し、これら双方が一致するか否かを判定する工程と、

(c-3-3)前記事業者設備が、前記工程(c-3-2)の2つの判定のいずれにおいても一致するとの判定結果を得たときに限って、前記変更を許可する工程と、

(c-3-4)前記工程(c-3-3)の後に、前記端末装置の前記補助部を交換し、交換後の補助部を前記本体部へ装着する工程と、

(c-3-5)前記端末装置が、前記工程(c-3-4)の後に、前記第1暗号化回路で暗号化された形式で、前記識別符号と交換後の前記補助部にもとづく変更後の前記記憶符号とを前記事業者設備へ送信する工程と、

(c-3-6)前記事業者設備が、前記工程(c-3-3)で前記変更を許可した場合に限って、受信した変更後の前記記憶符号を前記登録鍵にもとづいて復号化することにより得られる符号で、前記第2登録符号を更新する工程と、を備える、請求項45または請求項46に記載の通信方法。

【請求項48】 前記高位認証工程において、前記事業者設備は、前記高位の認証を行わない場合には、前記工程(c-2-2)で各登録符号との比較の対象とされた各符号を記録する、請求項42ないし請求項47のいずれかに記載の通信方法。

【請求項49】 前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合には、それ以前の通信に対する通信料金を、裏付けられたものとして記録する、請求項42ないし請求項48のいずれかに記載の通信方法。

【請求項50】 前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合に当該高位の認証を行ったことを記録し、

前記認証工程では、前記事業者設備は、前記高位の認証を行ったことが記録されていることをさらなる条件として、前記認証を行う、請求項42ないし請求項49のいずれかに記載の通信方法。

【請求項51】 前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合には、それ以前の通信によって行われた商取引が成立したものとして記録し、前記高位の認証を行わない場合には、それ以前の通信によって行われた前記商取引が成立しなかったものとして記録する、請求項42ないし請求項50のいずれかに記載の通信方法。

【請求項52】 前記認証工程において、前記事業者設備は、前記認証を行う場合には前記通信を継続し、前記認証を行わない場合には前記通信を中止する、請求項38ないし請求項51のいずれかに記載の通信方法。

【請求項53】 通信事業者設備を媒介した無線通信と前記通信事業者設備を媒介しない無線通信網の形成とが可能で、端末装置を携帯する群衆が集合ないし通行する空間において、前記群衆の中の少なくとも一部の複数人が携帯する前記端末装置の間で前記無線通信網を形成することにより、前記通信事業者設備を媒介した前記無線通信を行い得ない領域が前記空間の中にあっても、前記空間の中での前記端末装置どうしの通信を可能とした通信方法。

【請求項54】 前記無線通信網を形成する前記複数の端末装置の一部が、前記通信事業者設備を媒介した前記無線通信を行うことにより、前記無線通信網を形成する前記複数の端末装置の他の一部が、前記無線通信網を媒介しさらに前記通信事業者設備を媒介した通信をも行うことを可能とした、請求項53に記載の通信方法。

【請求項55】 前記無線通信網を形成する前記複数の端末装置の少なくとも一部であって、前記無線通信網を媒介して相互に通信する一組の端末装置が、それぞれを識別する符号を相互に交換することにより共通鍵を算出し、当該共通鍵にもとづいて暗号化した形式で通信信号をやりとりする、請求項53または請求項54に記載の通信方法。

【請求項56】 前記無線通信網を媒介した通信を、緊急非常通信に限って可能とした、請求項53ないし請求項55のいずれかに記載の通信方法。

【請求項57】 前記無線通信網の形成が可能で別の端末装置を、前記通信事業者設備を媒介した前記無線通信

を行い得ない前記領域に設置し、それにより、前記端末装置を携帯する前記群衆の密度が低い場合でも、前記無線通信網の形成を可能とした、請求項53ないし請求項56のいずれかに記載の通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、半導体装置、端末装置および通信方法に関する。

【0002】

【従来の技術】携帯電話機等の端末装置の不正使用、すなわち、識別番号を変更するなどにより、自己の端末装置を、通信ネットワークの中で、あたかも他人の端末装置であるかのように見せかけて、料金支払いの義務を逃れるなどの犯罪が、近年において増加していると云われている。この不正使用は、当然ながら他の犯罪と同様に、法律的な処罰を通じて社会的に規制されるべきものであるが、同時に、不正使用を行うことを技術的に困難なものとすること、すなわち不正使用に対する技術的障壁（セキュリティ）を高めることが、犯罪を防止する上で特に重要な対策の一つであると認識されている。

【0003】図64は、「日経エレクトロニクス」1999年2月8日号（no.736）、pp.155-162（以下、文献1）に掲載された記事から引用した説明図であり、携帯電話機に関して現在実施されている不正防止対策の一例を示している。文献1に記載されるように、図64の方法は、現行の不正防止対策の中で最もセキュリティの高い方法と云われており、「認証」という手順を利用している。

【0004】この方法では、携帯電話機のシリアル番号（ESN: Electronic Serial Number）、携帯電話機と通信事業者の認証センタとが共有する共有秘密データ（SSD: Shared Secret Data）、および、モバイル識別番号（MIN: Mobile Identification Number）が、携帯電話機ごとに付与される。これらの識別番号は、CAVE（Cellular Authentication and Voice Encryption）アルゴリズムにもとづいて、AUTHREQと称される暗号へと符号化される。暗号化の際に、通信事業者のモバイル交換センタから出力されるRANDと称される乱数が用いられる。

【0005】通信事業者は、携帯電話機から送信された暗号AUTHREQを、CAVEアルゴリズムにもとづいて復号化する。復号化されて得られた識別番号は、認証センタのみが把握する共有秘密データSSDを含む識別番号と比較され、その結果に応じて、通信の許可または不許可の判定がなされる。このように、携帯電話機と通信事業者との間でのみ共有される共有秘密データSSDにもとづいて、携帯電話機の使用者が正当使用者であるか否かのチェック、すなわち、認証が行われる。

【0006】

【発明が解決しようとする課題】しかしながら、現行の中で最も強力な不正防止対策であるとされる図64の認証方式に対しても、この認証をかわして不正使用を行う



という犯罪が、広がりつつあると云われている。その技術上の原因の一つが、文献1にも記載されるように、携帯電話機に付与される識別番号が、書き換え可能なフラッシュメモリ（フラッシュROM）に書き込まれていることにあると云われている。

【0007】図65は、携帯電話機の内部構成を簡単に示すブロック図である。従来の携帯電話機903には、通信回路907とともに、フラッシュメモリ908が備わっている。通信回路907は、フラッシュメモリ908に書き込まれたプログラムにしたがって動作する。識別番号もフラッシュメモリ908に保持されており、通信回路907は、フラッシュメモリ908から読み出された識別番号IDにもとづいて符号化を行い、符号化によって生成された暗号AUTHREQを通信事業者へ送信する。

【0008】記憶媒体として、書き換え可能なフラッシュメモリ908が用いられるのは、通信事業者が行うプログラム変更、例えば、新しい通信方式に対応したプログラムへの変更などに対応する必要があるためである。さらに、書き換え不能なマスクROMが用いられると、プログラム変更に対応できないだけでなく、マスクROMを製造する過程で、個体毎に異なる識別番号に対応した異なるマスクパターンを用いて、識別番号を記録する必要があり、製造効率の低下、および、製造コストの上昇がもたらされるからである。

【0009】本願出願人によって先になされた出願（特願平11-178173号；以下、文献2）は、多結晶体を有する半導体素子を半導体基板に形成し、多結晶体の結晶構造のばらつきに由来する電気的特性のばらつきを、識別番号の生成に利用することにより、上記した原因を除去する技術を開示している。

【0010】一方、端末装置の不正使用として、識別番号を書き換えることによって行われる形態だけでなく、端末装置に搭載されている半導体基板（半導体チップ）を不正に取り替えることによって行われる形態も知られている。すなわち、ある識別番号が記録された半導体基板を、別の識別番号が記録された半導体基板に取り替えることにより、自己の端末装置を他人の端末装置であるかのように見せかけて、料金支払いの義務を逃れる等の不正使用の形態も出現している。また、端末装置に限らず、例えば賭博性のある遊技機（我国において「パチンコ台」と通称される遊技機はその代表例）などをも含めた一般の半導体装置の応用機器において、半導体基板を取り替えて不正使用を行うことにより、不法利得を得るという犯罪も知られている。

【0011】さらに、通信事業者設備を媒介して無線通信を行う携帯可能な端末装置（すなわち携帯電話機）において、端末装置を使用していながら、その紛失を装って、料金支払いの義務を逃れるという不正使用の形態も知られている。

【0012】この発明は、従来の技術における上記した問題点を解消するためになされたもので、様々な形態での不正使用に対する技術的障壁を高めることのできる半導体装置、端末装置および通信方法を得ることを目的としており、さらに、これらの技術を利用することにより無線通信における利便性を高めた端末装置および通信方法を提供することを目的とする。

#### 【0013】

【課題を解決するための手段】第1の発明の装置は、半導体装置において、少なくとも一つの半導体基板の各々に形成され、その半導体基板に固有の識別符号を生成する符号生成部と、前記識別符号の各々ごとに、対応する半導体基板とは別の半導体基板に形成され、対応する識別符号に一致する符号を記憶符号として記憶するメモリと、を備える。

【0014】第2の発明の装置では、第1の発明の半導体装置において、前記メモリが、前記記憶符号を記憶するOTPROMを備える。

【0015】第3の発明の装置では、第1または第2の発明の半導体装置において、前記符号生成部が、半導体素子と、前記半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより、前記識別符号を生成し、出力する符号化回路と、を備える。

【0016】第4の発明の装置では、第3の発明の半導体装置において、前記半導体素子が多結晶体を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する。

【0017】第5の発明の装置では、第1または第2の発明の半導体装置において、前記符号生成部が、前記識別符号を記憶するOTPROMを備える。

【0018】第6の発明の装置は、第1ないし第5のいずれかの発明の半導体装置において、前記識別符号の各々ごとに、前記識別符号と、対応する前記記憶符号とを比較し、これら双方が一致するか否かを判定し、その結果を表現する判定信号を出力する比較回路を、さらに備える。

【0019】第7の発明の装置では、第6の発明の半導体装置において、前記比較回路が、比較対象とする識別符号に対応する前記半導体基板に形成されている。

【0020】第8の発明の装置は、第7の発明の半導体装置において、前記識別符号の各々ごとに、対応する前記半導体基板に形成された鍵生成部、暗号化回路および復号化回路を、さらに備え、前記鍵生成部は、対応する前記半導体基板に固有である暗号化のための鍵を生成し、前記暗号化回路は、対応する前記半導体基板に形成された前記符号生成部が生成する前記識別符号を、対応する前記鍵にもとづいて暗号化し、暗号化された形式で対応する前記メモリへ伝え、対応する前記メモリは、前記暗号化回路が出力する暗号化された形式での前記識別

符号を、暗号化された形式での前記記憶符号として記憶し、前記復号化回路は、対応する前記メモリに記憶される暗号化された前記記憶符号を、対応する前記鍵にもとづいて復号化し、前記比較回路は、対応する前記符号化回路が生成する前記識別符号と、対応する前記復号化回路が生成する復号化された前記記憶符号とを比較する。

【0021】第9の発明の装置では、第8の発明の半導体装置において、前記鍵生成部が、別の半導体素子と、前記別の半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより、前記鍵を生成し、出力する別の符号化回路と、を備える。

【0022】第10の発明の装置では、第9の発明の半導体装置において、前記別の半導体素子が多結晶性を有しており、前記別の半導体素子の前記電気的特性のばらつきが、前記多結晶性の結晶構造のばらつきに由来する。

【0023】第11の発明の装置では、第8の発明の半導体装置において、前記鍵生成部が、前記鍵を記憶するOTPROMを備える。

【0024】第12の発明の装置は、第7ないし第11のいずれかの発明の半導体装置において、前記識別符号の各々ごとに、対応する前記半導体基板に形成され、対応する前記符号化回路が生成した前記識別符号の、対応する前記メモリへの送出と、対応する前記メモリに記憶される前記記憶符号の前記比較回路への入力とを、排他的に行うスイッチ回路を、さらに備える。

【0025】第13の発明の装置は、第6ないし第12のいずれかの発明の半導体装置において、前記識別符号の各々に対応した前記判定信号に依存して選択的に動作または非動作となる回路部分を含む所定回路を、さらに備える。

【0026】第14の発明の装置では、第13の発明の半導体装置において、前記所定回路が、前記比較回路が形成されている前記少なくとも一つの半導体基板の一つに形成されている。

【0027】第15の発明の装置では、第1ないし第14のいずれかの発明の半導体装置において、前記少なくとも一つの半導体基板の個数が単一である。

【0028】第16の発明の装置では、第1ないし第14のいずれかにの発明の半導体装置において、前記少なくとも一つの半導体基板の個数が2個であり、前記識別符号の各々ごとに、対応する前記符号生成部と前記メモリは、互いに前記2個の半導体基板の一方と他方とに形成されている。

【0029】第17の発明の装置は、端末装置であって、半導体素子と当該半導体素子の電気的特性のばらつきに由来して値がばらつくように前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより暗号化のための鍵を生成し、出力する符号化回路とを備える

鍵生成部と、前記鍵にもとづいて送信データを暗号化する暗号化回路と、前記鍵にもとづいて受信データを復号化する復号化回路と、を備える。

【0030】第18の発明の装置では、第17の発明の端末装置において、前記符号化回路と前記復号化回路とが本体部に組み込まれており、前記鍵生成部が、前記本体部に脱着自在の補助部に組み込まれている。

【0031】第19の発明の装置では、第18の発明の端末装置において、前記補助部がICカードである。

【0032】第20の発明の装置では、第17ないし第19のいずれかの発明の端末装置において、前記半導体素子が多結晶性を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶性の結晶構造のばらつきに由来する。

【0033】第21の発明の装置は、端末装置であって、第13または第14の発明の半導体装置を備え、前記所定回路が、外部との間で信号を送信および受信する通信回路であって、前記判定信号の各々が前記識別符号の少なくとも一つと対応する前記記憶符号との間の不一致を示すときには、送信または受信の少なくとも一方を停止する。

【0034】第22の発明の装置は、端末装置であって、第6ないし第12のいずれかの発明の半導体装置と、外部との間で信号を送信および受信する通信回路と、を備え、前記通信回路は、前記信号の一部として前記判定信号の各々を前記外部へ送信する。

【0035】第23の発明の装置は、端末装置であって、第1ないし第5のいずれかの発明の半導体装置と、外部との間で信号を送信および受信する通信回路と、を備え、前記通信回路は、前記信号の一部として前記識別符号の各々と前記記憶符号の各々とを前記外部へ送信する。

【0036】第24の発明の装置では、第23の発明の端末装置において、前記少なくとも一つの半導体基板の個数が単一であって、前記符号生成部の各々と前記通信回路とが本体部に組み込まれており、前記メモリの各々が前記本体部に脱着自在の補助部に組み込まれている。

【0037】第25の発明の装置では、第24の発明の端末装置において、前記本体部には、暗号化のための第1鍵を生成する第1鍵生成部と、前記符号生成部が生成する前記識別符号を、前記第1鍵にもとづいて暗号化する第1暗号化回路と、がさらに組み込まれており、前記補助部には、暗号化のための第2鍵を生成する第2鍵生成部と、前記メモリが記憶する前記記憶符号を、前記第2鍵にもとづいて暗号化する第2暗号化回路と、がさらに組み込まれており、前記第1暗号化回路は、前記第2暗号化回路が暗号化した前記記憶符号をも、前記第1鍵にもとづいて暗号化し、前記通信回路は、前記第1暗号化回路で暗号化された形式で、前記識別符号および前記記憶符号を前記外部へ送信する。



【0038】第26の発明の装置では、第25の発明の端末装置において、前記第1鍵生成部と前記第1暗号化回路とが、前記符号化回路が形成された前記半導体基板に形成されている。

【0039】第27の発明の装置では、第25または第26の発明の端末装置において、前記第2鍵生成部と前記第2暗号化回路とが、前記メモリが形成された前記半導体基板に形成されている。

【0040】第28の発明の装置では、第24ないし第27のいずれかの発明の端末装置において、前記本体部が、充電可能な電池を備えており、前記補助部が、前記本体部に装着されることにより前記電池を充電する充電器である。

【0041】第29の発明の装置では、第24ないし第27のいずれかの発明の端末装置において、前記補助部がICカードであり、前記本体部と前記補助部の各々には、前記補助部から前記本体部への符号の伝送を無線で媒介するための通信インタフェースが、さらに組み込まれている。

【0042】第30の発明の装置では、第22ないし第29のいずれかの発明の端末装置において、前記通信回路が、前記少なくとも一つの半導体基板の一つに前記符号生成部とともに形成されている。

【0043】第31の発明の装置は、端末装置であって、通信事業者設備を媒介した無線通信を行う通信回路と、前記通信事業者設備を媒介しない無線通信網を形成することにより無線通信を行う無線通信網回路と、を備える。

【0044】第32の発明の装置は、第31の発明の端末装置において、前記通信回路と前記無線通信網回路との間での通信信号の経路の接続と切断とを選択自在に実行することにより、前記無線通信網を通じての前記端末装置の使用者と他者との間の通信と、前記無線通信網を通じての前記端末装置の使用者以外の複数の他者どうしの通信の中継と、を選択自在に実現する切替回路を、さらに備える。

【0045】第33の発明の装置は、第32の発明の端末装置において、暗号化のための鍵を生成する鍵生成部と、前記通信信号の中で前記通信回路から前記無線通信網回路へ送られる送信信号を前記鍵にもとづいて暗号化する暗号化回路と、前記通信信号の中で前記無線通信網回路から前記通信回路へ送られる受信信号を前記鍵にもとづいて復号化する復号化回路と、をさらに備え、前記鍵生成部が、前記端末装置を識別するための符号を生成する符号生成部と、前記符号生成部が生成する前記符号と、前記無線通信網回路を通じて通信相手から送られる別の符号とにもとづいて、前記使用者と前記通信相手との間で共通に使用可能な共通鍵を算出する鍵演算部と、を備える。

【0046】第34の発明の装置では、第33の発明の

端末装置において、前記符号生成部が、半導体素子と、前記半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより、前記符号を生成し、出力する符号化回路と、を備える。

【0047】第35の発明の装置では、第34の発明の端末装置において、前記半導体素子が多結晶体を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する。

【0048】第36の発明の装置では、第33の発明の端末装置において、前記符号生成部が、前記符号を記憶するOTPROMを備える。

【0049】第37の発明の装置は、第32ないし第36のいずれかの発明の端末装置において、前記通信信号の中で前記無線通信網回路から前記通信回路へ送られる受信信号の経路に介挿された第1および第2ミキサを、さらに備え、前記第1ミキサは、前記通信回路が受信した受信信号を復調し、前記第2ミキサは、復調された前記受信信号を前記通信回路の周波数帯域内の周波数を有する搬送波を用いて変調する。

【0050】第38の発明の方法は、事業者設備と第22の発明の端末装置とが相互に通信を行う通信方法であって、(a)前記端末装置が、前記判定信号の各々を前記事業者設備へ送信する工程と、(b)前記事業者設備が、受信した前記判定信号の各々が、前記識別符号の各々と対応する前記記憶符号との一致を示すという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備える。

【0051】第39の発明の方法は、事業者設備と第23の発明の端末装置とが相互に通信を行う通信方法であって、(a)前記端末装置が、前記識別符号の各々と前記記憶符号の各々を前記事業者設備へ送信する工程と、(b)前記事業者設備が、受信した前記識別符号の各々と対応する前記記憶符号と比較し、一致するか否かを判定する工程と、(c)前記事業者設備が、前記工程(b)において前記識別符号の各々が対応する前記記憶符号に一致すると判定したという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備える。

【0052】第40の発明の方法は、第39の発明の通信方法において、(e)前記事業者設備が、受信した前記識別符号の各々と前記記憶符号の各々を記録する工程を、さらに備える。

【0053】第41の発明の方法は、第39の発明の通信方法であって、前記工程(c)において、前記事業者設備は、前記認証を行わない場合には、受信した前記識別符号の各々と前記記憶符号の各々を記録する。

【0054】第42の発明の方法は、(a)事業者設備

が、第24の発明の端末装置の前記識別符号を得て、第1登録符号として記憶する工程と、(b)前記事業者設備が、前記端末装置の前記記憶符号を得て、第2登録符号として記憶する工程と、(c)前記工程(a)および(b)の後に、前記事業者設備と前記端末装置とが相互に通信を行う通信工程と、を備え、当該通信工程(c)は、(c-1)前記補助部が前記本体部に装着されていないときに実行される第1通信工程と、(c-2)前記補助部が前記本体部に装着されているときに実行される第2通信工程と、を備え、前記第1通信工程(c-1)は、(c-1-1)前記端末装置が、前記識別符号を前記事業者設備へ送信する工程と、(c-1-2)前記事業者設備が、受信した前記識別符号と前記第1登録符号とを比較し、これら双方が一致するか否かを判定する工程と、(c-1-3)前記事業者設備が、前記工程(c-1-2)で前記双方が一致すると判定したという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備え、前記第2通信工程(c-2)は、(c-2-1)前記端末装置が、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、(c-2-2)前記事業者設備が、受信した前記識別符号と前記第1登録符号とを比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号と前記第2登録符号とを比較し、これら双方が一致するか否かを判定する工程と、(c-2-3)前記事業者設備が、前記工程(c-2-2)の2つの判定のいずれにおいても一致するとの判定が得られたという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの高位の認証を行い、前記条件が充足されなければ、前記高位の認証を行わない高位認証工程と、を備える。

【0055】第43の発明の方法は、第42の発明の通信方法であって、前記工程(b)では、前記補助部が前記本体部に装着された状態で前記事業者設備と前記端末装置とが通信を行うことにより、事業者設備が、前記端末装置の前記記憶符号を得る。

【0056】第44の発明の方法では、第42または第43の発明の通信方法において、前記工程(c)が、(c-3)前記補助部が前記本体部に装着されているときに実行され、前記第2登録符号の変更を行う変更工程を、さらに備え、前記変更工程(c-3)は、(c-3-1)前記端末装置が、前記変更の意志を表現する要求信号とともに、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、(c-3-2)前記事業者設備が、受信した前記識別符号と前記第1登録符号とを比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号と前記第2登録符号とを比較し、これら双方が一致するか否かを判定する工程と、(c-3-3)前記事業者設備が、前記工程(c-3-2)の2つの判定のいずれにおいても一致するとの判定結果を得たときに限って、前記変更を許可する工程と、(c-3-4)前記工程(c-3-3)の後に、前記端末装

置の前記補助部を交換し、交換後の補助部を前記本体部へ装着する工程と、(c-3-5)前記端末装置が、前記工程(c-3-4)の後に、前記識別符号と交換後の前記補助部にもとづく変更後の前記記憶符号とを前記事業者設備へ送信する工程と、(c-3-6)前記事業者設備が、前記工程(c-3-3)で前記変更を許可した場合に限って、受信した変更後の前記記憶符号で前記第2登録符号を更新する工程と、を備える。

【0057】第45の発明の方法は、(a)事業者設備が、第25の発明の端末装置の前記識別符号および前記第1鍵を得て、それぞれ第1登録符号および登録鍵として記憶する工程と、(b)前記事業者設備が、前記端末装置の前記第2鍵で暗号化された前記記憶符号を得て、第2登録符号として記憶する工程と、(c)前記工程(a)および(b)の後に、前記事業者設備と前記端末装置とが相互に通信を行う通信工程と、を備え、当該通信工程(c)は、(c-1)前記補助部が前記本体部に装着されていないときに実行される第1通信工程と、(c-2)前記補助部が前記本体部に装着されているときに実行される第2通信工程と、を備え、前記第1通信工程(c-1)は、(c-1-1)前記端末装置が、前記第1暗号化回路で暗号化された形式で、前記識別符号を前記事業者設備へ送信する工程と、(c-1-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第1登録符号と比較し、これら双方が一致するか否かを判定する工程と、(c-1-3)前記事業者設備が、前記工程(c-1-2)で前記双方が一致すると判定したという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備え、前記第2通信工程(c-2)は、(c-2-1)前記端末装置が、前記第1暗号化回路で暗号化された形式で、前記識別符号および記憶符号を前記事業者設備へ送信する工程と、(c-2-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第1登録符号と比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号を前記登録鍵にもとづいて復号化した上で、前記第2登録符号と比較し、これら双方が一致するか否かを判定する工程と、(c-2-3)前記事業者設備が、前記工程(c-2-2)の2つの判定のいずれにおいても一致するとの判定が得られたという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの高位の認証を行い、前記条件が充足されなければ、前記高位の認証を行わない高位認証工程と、を備える。

【0058】第46の発明の方法は、第45の発明の通信方法であって、前記工程(b)では、前記補助部が前記本体部に装着された状態で前記事業者設備と前記端末装置とが通信を行うことにより、事業者設備が、前記端末装置の前記第2鍵で暗号化された前記記憶符号を得る。

【0059】第47の発明の方法では、第45または第

46の発明の通信方法において、前記工程(c)が、(c-3)前記補助部が前記本体部に装着されているときに実行され、前記第2登録符号の変更を行う変更工程を、さらに備え、前記変更工程(c-3)は、(c-3-1)前記端末装置が、前記変更の意志を表現する要求信号とともに、前記第1暗号化回路で暗号化された形式で、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、(c-3-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第1登録符号と比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号を前記登録鍵にもとづいて復号化した上で、前記第2登録符号と比較し、これら双方が一致するか否かを判定する工程と、(c-3-3)前記事業者設備が、前記工程(c-3-2)の2つの判定のいずれにおいても一致するとの判定結果を得たときに限って、前記変更を許可する工程と、(c-3-4)前記工程(c-3-3)の後に、前記端末装置の前記補助部を交換し、交換後の補助部を前記本体部へ装着する工程と、(c-3-5)前記端末装置が、前記工程(c-3-4)の後に、前記第1暗号化回路で暗号化された形式で、前記識別符号と交換後の前記補助部にもとづく変更後の前記記憶符号とを前記事業者設備へ送信する工程と、(c-3-6)前記事業者設備が、前記工程(c-3-3)で前記変更を許可した場合に限って、受信した変更後の前記記憶符号を前記登録鍵にもとづいて復号化することにより得られる符号で、前記第2登録符号を更新する工程と、を備える。

【0060】第48の発明の方法は、第42ないし第47のいずれかの発明の通信方法であって、前記高位認証工程において、前記事業者設備は、前記高位の認証を行わない場合には、前記工程(c-2-2)で各登録符号との比較の対象とされた各符号を記録する。

【0061】第49の発明の方法は、第42ないし第48のいずれかの発明の通信方法であって、前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合には、それ以前の通信に対する通信料金を、裏付けられたものとして記録する。

【0062】第50の発明の方法は、第42ないし第49のいずれかの発明の通信方法であって、前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合に当該高位の認証を行ったことを記録し、前記認証工程では、前記事業者設備は、前記高位の認証を行ったことが記録されていることをさらなる条件として、前記認証を行う。

【0063】第51の発明の方法は、第42ないし第50のいずれかの発明の通信方法であって、前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合には、それ以前の通信によって行われた商取引が成立したものとして記録し、前記高位の認証を行わない場合には、それ以前の通信によって行われた前記商取引が成立しなかったものとして記録する。

【0064】第52の発明の方法は、第38ないし第51のいずれかの発明の通信方法であって、前記認証工程において、前記事業者設備は、前記認証を行う場合には前記通信を継続し、前記認証を行わない場合には前記通信を中止する。

【0065】第53の発明の方法は、通信方法であって、通信事業者設備を媒介した無線通信と前記通信事業者設備を媒介しない無線通信網の形成とが可能な端末装置を携帯する群衆が集合ないし通行する空間において、前記群衆の中の少なくとも一部の複数人が携帯する前記端末装置の間で前記無線通信網を形成することにより、前記通信事業者設備を媒介した前記無線通信を行い得ない領域が前記空間の中にあっても、前記空間の中での前記端末装置どうしの通信を可能とする。

【0066】第54の発明の方法は、第53の発明の通信方法において、前記無線通信網を形成する前記複数の端末装置の一部が、前記通信事業者設備を媒介した前記無線通信を行うことにより、前記無線通信網を形成する前記複数の端末装置の他の一部が、前記無線通信網を媒介しさらに前記通信事業者設備を媒介した通信をも行うことを可能とする。

【0067】第55の発明の方法では、第53または第54の発明の通信方法において、前記無線通信網を形成する前記複数の端末装置の少なくとも一部であって、前記無線通信網を媒介して相互に通信する一組の端末装置が、それぞれを識別する符号を相互に交換することにより共通鍵を算出し、当該共通鍵にもとづいて暗号化した形式で通信信号をやりとりする。

【0068】第56の発明の方法は、第53ないし第55のいずれかに記載の通信方法において、前記無線通信網を媒介した通信を、緊急非常通信に限って可能とする。

【0069】第57の発明の方法は、第53ないし第56のいずれかに記載の通信方法において、前記無線通信網の形成が可能な別の端末装置を、前記通信事業者設備を媒介した前記無線通信を行い得ない前記領域に設置し、それにより、前記端末装置を携帯する前記群衆の密度が低い場合でも、前記無線通信網の形成を可能とする。

【0070】

【発明の実施の形態】はじめに、本明細書で用いる用語について説明する。本明細書において、符号に関して「一致」とは、完全一致に限定されず、あらかじめ定められた範囲内での近似をも包含する。

【0071】[1. 実施の形態1] 実施の形態1では、2個の半導体基板の一方に固有の識別符号を他方に記憶させておくことにより、半導体基板を取り替えて行われる不正使用を防止する半導体装置、およびその応用機器としての端末装置について説明する。

【0072】[1.1. 半導体装置] 図1は、実施の形態

1による半導体装置の構成を示すブロック図である。この半導体装置600は、符号生成部400、比較回路403および所定回路405、およびメモリ601を備えている。符号生成部400、比較回路403および所定回路405は、半導体基板CH1に形成されており、メモリ601は別の半導体基板CH2に形成されている。半導体基板CH1、CH2は、モールドされた形態およびベアチップのいずれであってもよく、単一または複数の回路基板の上に搭載されている。

【0073】符号生成部400は、半導体基板CH1に固有の識別符号Cdを生成する。メモリ601は、符号生成部400が生成した識別符号Cdを記憶符号Coとして記憶する。識別符号Cdは、半導体装置600が製品として出荷されるときに、符号生成部400からメモリ601へ送信され、メモリ601へ書き込まれる。

【0074】比較回路403は、符号生成部400が生成する識別符号Cdとメモリ601から読み出された記憶符号Coとを比較し、これら双方が互いに一致するかどうかを判定し、その結果を表現する判定信号Enを出力する。一致性の判定として、完全一致性を判定するのであれば、比較回路403は、双方の符号の差がゼロであるかどうかを判定する従来周知のコンパレータを備えれば足りる。あらかじめ定められた範囲内での近似性を判定するのであれば、比較回路403は、双方の符号の差の大きさを、一定の基準値と比較すればよい。差の大きさは、例えば、数値としての差の大きさ、あるいは互いに相違するビット数で評価することが可能である。また、基準値を外部から入力可能とし、半導体装置600のユーザが所望の値に基準値を設定できるように、半導体装置600を構成することも可能である。

【0075】所定回路405は、所定の機能を果たすべく複数の回路素子によって形成された回路であり、比較回路403が出力する判定信号Enにもとづいて選択的に動作または非動作となる回路部分を含んでいる。図65に示した通信回路907は、所定回路405の一例となり得る。

【0076】半導体装置600は以上のように構成されるので、符号生成部400が生成する識別符号Cdとメモリ601から読み出される記憶符号Coとが互いに一致したときのみ、所定回路405のすべての部分が動作する。したがって、所定回路405を応用機器の機能を実現する回路の一部とすることにより、比較の結果に応じて、応用機器の所定の動作を許可および不許可することができる。半導体基板CH1またはCH2を、別の半導体基板に取り替えて応用機器を不正に使用しようとしても、識別符号Cdと記憶符号Coとが一致しないので、応用機器は所定の動作をなし得ない。半導体装置600が組み込まれた応用機器は、このようにして半導体基板の取り替えによる不正使用を防止することができる。

【0077】符号生成部400と比較回路403とが単一の半導体基板CH3に形成され、所定回路405はそれとは別の半導体基板に形成されても良い。しかしながら、所定回路405が符号生成部400および比較回路403とともに、単一の半導体基板CH1に形成される形態では、比較回路403から所定回路405へ入力される判定信号Enを、外部から入力することができない。このため、不正使用に対する障壁がさらに高められるという利点が得られる。

【0078】また、符号生成部400が形成される半導体基板とは別の半導体基板に比較回路403が形成されても良い。しかしながら、比較回路403が符号生成部400とともに単一の半導体基板CH1またはCH3に形成される形態では、符号生成部400から比較回路403へ入力される識別符号Cdを外部から不正に変更することができない。このため、不正使用に対する障壁が、さらに高められるという利点が得られる。

【0079】さらに、半導体装置600が所定回路405を備えない形態を実施することも可能である。この場合には、所定回路405を、半導体装置600とは別個に、応用機器に形成すると良い。あるいは、判定信号Enを応用機器の外部へ取り出し、その値に応じて、外部から応用機器の動作、非動作を指示することができるように、応用機器を構成することも可能である。後述する実施の形態3の端末装置はそのような応用機器の一例である。

【0080】また、半導体装置600が所定回路405も比較回路403も備えない形態を実施することも可能である。この場合には、所定回路405および比較回路403を、半導体装置600とは別個に、応用機器に形成すると良い。あるいは、識別符号Cdと記憶符号Coとを応用機器の外部へ取り出し、その値に応じて、外部から応用機器の動作、非動作を指示することができるように、応用機器を構成することも可能である。後述する実施の形態4の端末装置はそのような応用機器の一例である。

【0081】[1.2. 符号生成部] 図2は、符号生成部400の内部構成の好ましい一例を示すブロック図である。図2の例では、符号生成部400は、半導体素子401および符号化回路402を備えている。符号化回路402は、半導体素子401の電気的特性をアナログ信号Anとして読み出し、デジタル信号へ変換する。変換によって得られたデジタル信号は、識別符号Cdとして出力される。

【0082】半導体素子401の電気的特性として、半導体素子401の個体毎にばらつきを持った特性が選ばれる。それにより、識別符号Cdは、半導体素子401の個体毎にばらついた値として生成されるので、符号生成部400が形成されている半導体基板に固有の識別符号としての性格を備えることとなる。量産される多数の

半導体装置600の間で、同一工程で製造された半導体素子401を用いることができるので、半導体装置600の製造を簡略化することができる。また、識別符号Cdのもとになる半導体素子401の電気的特性を外部から変更することができないので、識別符号Cdの不正な変更に対する障壁が高いという利点も得られる。

【0083】電気的特性として、半導体装置401が多結晶性を備え、その結晶構造のばらつきに由来してばらつく特性を利用することが可能である。この例については、以下の図3～図6で詳述する。また、半導体素子401がMOSFETを備え、その不純物拡散層の不純物濃度のばらつきに起因するしきい値のばらつきを利用することも可能である。

【0084】図3は、半導体素子401の好ましい一例を示す平面図である。図4は、図3のA-A切断線に沿った断面図である。この例では、半導体素子401は、薄膜トランジスタ（以下、TFTと略記する）101を有しており、しかも、そのチャネル領域を含む半導体層1060が、多結晶性として形成されている。なお、図3には、説明の便宜のために半導体素子401の製造工程の中で中間生成物として形成される半導体層1を描いているが、製造工程の中で選択的エッチングが施されることにより、完成品としての半導体素子401では、半導体層1は半導体層1060へと成型されている。

【0085】TFT101では、絶縁膜12の上にゲート電極11が選択的に形成されており、絶縁膜12およびゲート電極11の表面全体が絶縁膜10で覆われている。絶縁膜10の上には、半導体層1が形成されている。各要素の材料の一例を述べると、絶縁膜12はシリコン酸化物であり、ゲート電極11は不純物がドーブされたポリシリコンであり、絶縁膜10はTEOSなどのシリコン酸化物であり、半導体層1の主成分はシリコンである。

【0086】半導体層1には、ゲート電極11の上部に位置するチャネル領域2、ならびに、このチャネル領域2を挟むソース領域3およびドレイン領域4が、形成されている。チャネル領域2に接する絶縁膜10の部分は、ゲート絶縁膜として機能する。図3および図5の例では、チャネル領域2の導電型は、n型であり、ソース領域3およびドレイン領域4の導電型は、p型である。すなわち、TFT101は、一例として、pチャネル型のMOS型TFTとして形成されている。いうまでもなく、TFT101は、nチャネル型のMOS型TFTとして形成されても良い。

【0087】半導体層1は、多結晶半導体層として形成されており、図3が示すように、無数の結晶粒（グレイン）5、および、それらの境界面に位置し結晶の乱れを生じている部分である結晶粒界（グレインバウンダリ）6を含んでいる。単一の結晶粒5の中では、結晶方位は一樣であるが、異なる結晶粒5の間では、結晶方位は一

般に異なる。また、結晶粒5の大きさおよび配置はランダムであり、半導体層1を形成する過程で、さまざまにばらつく。すなわち、多数のTFT101が同一の製造工程を通じて製造されても、TFT101の個体ごとに、半導体層1の結晶構造は異なったものとなる。

【0088】その結果、図5に例示するように、TFT101を仮に一つの個体を表すものとし、これと同一の製造工程で生産された別の個体をTFT102として、TFT101から仮に区別すると、チャネル領域2を占める結晶粒界6の量は、TFT101とTFT102の間で同一とはならない。図5は、半導体素子101よりもTFT102の方が、チャネル領域2に結晶粒界6を少なく含む例を示している。

【0089】多結晶TFTでは、チャネル領域2に含まれる結晶粒界6の量によって、その特性がばらつくことが知られている。この事実は、例えば、IEEE Transactions on Electron Devices, Vol. 45, No. 1, January (1998), pp. 165-172（以下、文献3）に記載されている。すなわち、図6にTFT101および102に関して、ゲート電圧Vgとドレイン電流Idとの間の関係を示すように、チャネル領域2に結晶粒界6を多く含むTFT101では、結晶粒界6を少なく含むTFT102に比べて、同一のゲート電圧Vg0の下でのドレイン電流Idが小さくなる（すなわち、 $I_{da} < I_{db}$ ）。

【0090】したがって、TFT101が有する多結晶性の結晶構造のばらつきを、半導体基板の識別に利用することが可能となる。個体間で異なる電気的特性は、多結晶性の結晶構造のばらつきに由来するために、フラッシュメモリ908（図65）へ記録された識別番号とは異なり、外部から書き換えることはできない。したがって、応用機器の不正利用に対するセキュリティを高めることができる。

【0091】しかも、フラッシュメモリ908へ識別番号をプログラムする技術とは異なり、プログラムを行う手間を必要としない。さらに、マスクROMに識別番号を記録する技術とは異なり、個体毎に異なる特性が同一の製造工程を通じて得られるので、製造工程が単純であり、製造工数および製造コストが低く抑えられる。さらに、多結晶性の結晶構造のばらつきは大きく、それによって電気的特性のばらつきも大きい。このため、識別符号Cdのばらつきの幅を広く確保することが可能である。すなわち、量産される多数の半導体装置600の間で、互いに識別符号が一致しないようにすることが容易である。

【0092】なお、製造工程が複雑にはなるが、TFT101のチャネル領域2のみが多結晶半導体で形成され、ソース領域3およびドレイン領域4は単結晶半導体で形成されていてもよく、この場合でも同様に、特性はランダムにばらつく。

【0093】図2～図6に示した半導体素子401の電



気的特性は、温度、時間の変化にともなって、微小ながら変化することも有り得る。それにともなって、識別符号C dは、完全な意味で一定の値を保持するとは限らず、ある程度の変動を伴うことも想定される。これに対処するためには、比較回路403は、識別符号C dの変動をも考慮した許容範囲内で、符号の一致性を判定するとよい。

【0094】半導体素子401が多結晶体を備える例として、図3～図6に示したTFTだけでなく、多結晶体を備える抵抗素子、多結晶体を備える容量素子など、他の素子の例を実施することも可能である。また、半導体素子401は、TFT等を複数個備えていても良い。TFT等の個数が多いほど、識別符号C dのばらつきの幅が拡大する。これらの例については、実施の形態12において詳細に説明する。

【0095】[1.3. OTPROMを用いた例] 図7は、符号生成部400の内部構成の好ましい別の一例を示すブロック図である。図7の例では、符号生成部400は、一回に限り書込が可能な不揮発性メモリであるOTP (One Time Programable) ROM602を備えている。半導体装置600が出荷されるときに、OTPROM602には識別符号C dが書き込まれる。その後、半導体装置600が使用者の手に渡った後に、OTPROM602に書き込まれている識別符号C dを、書き換えることは技術的に不可能である。すなわち、図7の例においても、符号生成部400が生成する識別符号C dの不正な変更に対する技術的障壁が高いという利点を得られる。

【0096】OTPROMは、符号生成部400だけでなく、図8が示すように、メモリ601への利用にも適している。図8の例では、メモリ601はOTPROM602を備えている。半導体装置600が出荷されるときに、メモリ601に備わるOTPROM602には、符号生成部400から送信される識別符号C dが、記憶符号C oとして書き込まれる。その後、半導体装置600が使用者の手に渡った後に、OTPROM602に書き込まれている記憶符号C oを、書き換えることは技術的に不可能である。すなわち、図8の例では、メモリ601に記憶される記憶符号C oの不正な変更に対する技術的障壁が高いという利点を得られる。それにより、符号生成部400が形成された半導体基板を取り替え、それと同時にメモリ601に記憶される記憶符号C oを、新たな半導体基板の識別符号C dに一致するように書き換えて行われる不正使用をも防止することができる。

【0097】[1.4. 端末装置] 図9は、半導体装置600の応用機器としての端末装置の構成を示すブロック図である。この端末装置1001は、携帯電話機として構成されている。端末装置1001が備える半導体装置1002は、図1に示した半導体装置600の一例であり、所定回路405として通信回路405aを備えてい

る。

【0098】好ましくは、符号生成部400、比較回路403および通信回路405aは、単一の半導体基板CH100に形成されるが、比較回路403および符号生成部400のみが単一の半導体基板CH102に形成されても良く、符号生成部400のみが単一の半導体基板に形成されてもよい。いずれの場合であっても、記憶符号C oを記憶するメモリ654は、符号生成部400が形成される半導体基板とは異なる半導体基板CH51に形成される。

【0099】端末装置1001の通信を媒介する事業者の設備である通信事業者（必要に応じて、「局」と略記する）設備655には、通信回路656が備わっている。通信回路405aと通信回路656との間で、音声、データなどを内容とする通信信号が、無線（すなわち電波）を媒介としてやり取りされる。端末装置1001と通信事業者設備655とによって、通信システム1000が構成される。

【0100】図10は、通信回路405aの内部構成の一例を示すブロック図である。無線を媒介する端末装置1001が備える通信回路405aでは、アンテナと信号処理回路（ベースバンド回路）800の間には、周知の無線周波回路462および中間周波回路463が介在する。信号処理回路800には、送信回路460と受信回路461とが備わっており、通信信号D tは受信回路461によって受信され、送信回路406によって送信される。

【0101】図10の例では、送信回路460のみが判定信号E nによってオン・オフする。すなわち、比較回路403が符号の不一致を判定すると、送信機能が停止する。受信回路461のみ、あるいは送信回路460と受信回路461の双方が、判定信号E nにもとづいてオン・オフするように通信回路405を構成することも可能である。

【0102】図11は、端末装置1001が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置600（より特定的には、半導体装置1001）が製造される（S201）。その最終工程、ないしそれ以前に、識別符号C dがメモリ601へ記憶符号C oとして記録される（S202）。その後、半導体装置600が電話機メーカーへ納入され、電話機メーカーによって端末装置1001が組み立てられる（S203）。完成した端末装置1001は、使用者（ユーザ）へ供給された後（S204）、使用者による通信への利用に供される（S205）。

【0103】ステップS206～S210は、端末装置1001を用いた通信の手順、すなわちステップS205の内部フローを表している。通信が開始されると、端末装置1001は、記憶符号C oをメモリ601から読み出す（S206）。つぎに、比較回路403によ



て、識別符号C dと記憶符号C oとの比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号E nが生成される(S 207)。

【0104】判定信号E nが符号の一致を示すときには(S 208)、通信回路405aは通信機能を維持することにより、通信処理を続行する(S 209)。一方、判定信号E nが符号の不一致を示すときには(S 208)、通信回路405aは送信機能または受信機能の少なくとも一方を停止することにより、通信を不能にする(S 210)。通信が完了すると、処理は終了する。

【0105】以上のように、端末装置1001では、判定信号E nが符号の不一致を示すときには、通信回路405aの少なくとも一部の機能が停止するので、半導体基板を取り替えて通信に使用するという不正行為が、通信事業者設備655による処理を待つことなく、端末装置1001それ自体の働きによって自動的に抑えられる。

【0106】なお、以上の説明では、端末装置として無線を通信媒体とする携帯電話機を例としたが、通信ケーブルを通信媒体とする有線の電話機に対しても、本実施

の形態は、同様に適用可能である。また、電話機に限らず様々な端末装置に対しても適用可能である。

【0107】図12は、本実施の形態が適用可能な様々な端末装置、および、端末装置が通信の対象とする事業者設備(サーバ)を例示している。例えば、端末装置は、高速道路の使用料金の支払い等を自動的に管理する高速道路管理システムと通信する自動車端末であってもよく、銀行のATMシステムと通信して現金の引き出し・預金等を行うICカードあるいはパーソナルコンピュータであってもよい。

【0108】[2. 実施の形態2] 実施の形態2では、実施の形態1の半導体装置および端末装置において、固有の識別符号で識別される半導体基板の個数が単数から複数へ拡張された形態について説明する。

【0109】図13は、実施の形態2による半導体装置の構成を示すブロック図である。図13が示す半導体装置620では、半導体基板CH4に符号生成部400、比較回路403および所定回路405の他に、メモリ601が形成されており、別の半導体基板CH5にはメモリ601の他に、符号生成部400および比較回路403が形成されている。半導体基板CH4に形成された符号生成部400は、半導体基板CH4に固有の識別符号C d1を生成し、半導体基板CH5に形成された符号生成部400は、半導体基板CH5に固有の識別符号C d2を生成する。

【0110】半導体基板CH4に形成されたメモリ601は、半導体基板CH5に形成された符号生成部400から送信される識別符号C d2を記憶符号C o2として記憶し、半導体基板CH5に形成されたメモリ601は、半導体基板CH4に形成された符号生成部400か

ら送信される識別符号C d1を記憶符号C o1として記憶する。すなわち、二つの半導体基板CH4、CH5のそれぞれに固有の識別符号C d、C d2が、他方の半導体基板に形成されたメモリ601に記憶される。

【0111】半導体基板CH4に形成された比較回路403は、識別符号C d1と記憶符号C o1とを比較し、半導体基板CH5に形成された比較回路403は、識別符号C d2と記憶符号C o2とを比較する。半導体基板CH4に形成された所定回路405は、二つの比較回路403が出力する判定信号E n1、E n2の組にもとづいて、選択的に動作または非動作となる回路部分を含んでいる。所定回路405は、例えば図10の通信回路405aにおいて、判定信号E n1、E n2のいずれか一方が符号の不一致を示しているときには、送信回路560は動作を停止するように構成することができる。それによって、半導体基板の取り替えによる不正使用に対する障壁をさらに高めることが可能となる。

【0112】固有の識別符号C dが付与される半導体基板の個数を、3個以上に拡張することも可能である。例えば、3個の半導体基板のそれぞれに、固有の識別符号C dを生成する符号生成部400とメモリ601とが形成され、メモリ601は、それ自身が形成されている半導体基板とは別の半導体基板に形成された符号生成部400から送信される識別符号C dを記憶するように半導体装置を構成しても良い。あるいは、3個のメモリ601の少なくとも一部を、符号生成部400が形成されている3個の半導体基板とは別の半導体基板に形成しても良い。

【0113】識別符号C dが付与された半導体基板、すなわち符号生成部400を備える半導体基板の個数が多いほど、応用機器の不正使用に対する障壁を、より高めることができる。また、メモリ601を符号生成部400を備える半導体基板にのみ形成することによって、半導体基板の個数を最小に抑えることができる。特に、図13に示した半導体装置620では、半導体基板の個数を、図1に示した半導体装置600における半導体基板の個数と同等の2個に抑えつつ、不正使用に対する障壁を高めることができるという利点が見られる。

【0114】図14は、半導体装置620の応用機器としての端末装置の構成を示すブロック図である。この端末装置1011は、携帯電話機として構成されており、通信事業者設備655とともに、通信システム1010を構成する。端末装置1011が備える半導体装置1012は、図13に示した半導体装置620の一例であり、所定回路405として通信回路405aを備えている。通信回路405aは、判定信号E n1、E n2のいずれかが、符号の不一致を示すときには、その一部の機能を停止する。

【0115】好ましくは、識別符号C d1を生成する符号生成部400、識別符号C d1を比較対象とする比較

回路403、記憶符号C02を記憶するメモリ601および通信回路405aは、単一の半導体基板CH103に形成されるが、比較回路403、メモリ601および符号生成部400のみが単一の半導体基板CH11に形成されても良く、符号生成部400のみが単一の半導体基板CH104に形成されてもよい。また、好ましくは、記憶符号C01を記憶するメモリ601は、識別符号Cd2を生成する符号生成部400、および識別符号Cd2を比較の対象とする比較回路403とともに、単一の半導体基板CH13に形成される。

【0116】図15は、端末装置1011が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置620（より特定的には、半導体装置1012）が製造される（S241）。その最終工程、ないしそれ以前に、各半導体基板の識別符号Cd1、Cd2が、他方の半導体基板のメモリ601へ記憶符号C01、C02として記録される（S242）。その後、半導体装置620が電話機メーカーへ納入され、電話機メーカーによって端末装置1011が組み立てられる（S243）。完成した端末装置1011は、使用者へ供給された後（S244）、使用者による通信への利用に供される（S245）。

【0117】ステップS246～S250は、端末装置1011を用いた通信の手順、すなわちステップS245の内部フローを表している。通信が開始されると、端末装置1011は、記憶符号C01およびC02を二つのメモリ601から読み出す（S246）。つぎに、一方の比較回路403によって、識別符号Cd1と記憶符号C01との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号En1が出力されると同時に、他方の比較回路403によって、識別符号Cd2と記憶符号C02との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号En2が出力される（S247）。

【0118】判定信号En1、En2のいずれもが、符号の一致を示すときには（S248）、通信回路405aは通信機能を維持することにより、通信処理を続行する（S249）。一方、判定信号En1、En2のいずれかが、符号の不一致を示すときには（S248）、通信回路405aは送信機能または受信機能の少なくとも一方を停止することにより、通信を不能にする（S250）。通信が完了すると、処理は終了する。

【0119】[3. 実施の形態3] 実施の形態3では、実施の形態1または2による半導体装置の中で、所定回路を除いた部分を利用した端末装置について説明する。

【0120】図16は、実施の形態3による端末装置の構成を示すブロック図である。この端末装置1001は、通信回路405aが比較回路403から送られる判定信号Enにもとづいて動作または非動作を選択的に行うのではなく、判定信号Enを通信信号の一部として通

信事業者設備655へ、単に送信する点において、図9に示した実施の形態1の端末装置1001とは特徴的に異なっている。

【0121】図16の端末装置1001が通信への利用に供されるまでの処理の流れは、図11のフローチャートと同等に描かれる。ただし、ステップS205の内部フローは、図17のステップS1000の処理へ置き換えられる。ステップS1000の処理が開始されると、端末装置1001は、記憶符号C0をメモリ601から読み出す（S206）。つぎに、比較回路403によって、識別符号Cdと記憶符号C0との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号Enが生成される（S207）。

【0122】この判定信号Enは、通信回路405aを通じて通信事業者設備655へ送信される（S208、S1001、S1003）。言い換えると、判定信号Enが符号の一致を示すときには（S208）、判定信号Enとして符号の一致を示す所定の値が送信され（S1001）、判定信号Enが符号の不一致を示すときには（S208）、上記所定の値は送信されない（S1003）。

【0123】通信事業者設備655は、判定信号Enが符号の一致を示すときには、端末装置1001の使用者が正当使用者であるとの認証を行い、判定信号Enが符号の不一致を示すときには、認証を行わない。通信事業者設備655は、例えば、認証を行うときには通信を許可して通信処理を続行し（S1002）、認証を行わないときには、通信を不許可として、通信処理を中止する（S1004）。

【0124】このように、図16の端末装置1001では、判定信号Enを通信事業者設備655の側で行われる認証処理の判断材料に供することができ、それにより、半導体基板の取り替えによる不正使用を認証の対象から排除して、精度の高い認証を実現することができる。なお、認証処理にともなう処理として、通信の継続または中止以外に、商取引の許可または不許可など、何らかのサービスの提供または不提供を行うことが可能である。あるいは、単に認証の判断材料を記録しておくという処理を行っても良い。これらの具体例については、後の実施の形態で説明する。

【0125】図18は、実施の形態3による端末装置の別の構成例を示すブロック図である。この端末装置10011は、通信回路405aが比較回路403から送られる判定信号En1、En2にもとづいて動作または非動作を選択的に行うのではなく、判定信号En1、En2を通信信号の一部として通信事業者設備655へ、単に送信する点において、図14に示した実施の形態1の端末装置1011とは特徴的に異なっている。

【0126】図18の端末装置1011が通信への利用に供されるまでの処理の流れは、図15のフローチャー

トと同等に描かれる。ただし、ステップS245の内部フローは、図19のステップS1010の処理へ置き換えられる。ステップS1010の処理が開始されると、端末装置1011は、記憶符号C01、C02を二つのメモリ601から読み出す(S246)。つぎに、一方の比較回路403によって、識別符号Cd1と記憶符号C01との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号En1が生成される。それと同時に、他方の比較回路403によって、識別符号Cd2と記憶符号C02との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号En2が生成される。(S247)。

【0127】これらの判定信号En1、En2は、通信回路405aを通じて通信事業者設備655へ送信される(S248、S1001、S1003)。言い換えると、判定信号En1、En2のいずれもが、符号の一致を示すときには(S248)、判定信号En1、En2として符号の一致を示す所定の値が送信され(S1001)、判定信号En1、En2のいずれかが、符号の不一致を示すときには(S208)、上記所定の値は送信されない(S1003)。

【0128】通信事業者設備655は、判定信号En1、En2のいずれもが、符号の一致を示すときには、端末装置1001の使用者が正当使用者であるとの認証を行い、判定信号En1、En2のいずれかが符号の不一致を示すときには、認証を行わない。通信事業者設備655は、例えば、認証を行うときには通信を許可して通信処理を続行し(S1002)、認証を行わないときには、通信を不許可として、通信処理を中止する(S1004)。

【0129】このように、図18の端末装置1001では、判定信号En1、En2を通信事業者設備655の側で行われる認証処理の判断材料に供することができ、それにより、半導体基板の取り替えによる不正使用を認証の対象から排除して、精度の高い認証を実現することができる。また、二つの判定信号En1、En2が判断材料とされるので、図16の端末装置1001よりもさらに、認証の精度を高めることができる。

【0130】[4. 実施の形態4] 実施の形態4では、実施の形態1または2による半導体装置の中で、所定回路および比較回路の双方を除いた部分を利用した端末装置について説明する。

【0131】図20は、実施の形態4による端末装置の構成を示すブロック図である。この端末装置801が備える半導体装置652は、比較回路403が除去され、通信回路405aが識別符号Cdおよび記憶符号Coを通信信号の一部として通信事業者設備655へ、単に送信する点において、図9に示した実施の形態1の半導体装置1002とは特徴的に異なっている。

【0132】図20の通信事業者設備655は、通信回

路656に加えて、判定回路657および顧客データメモリ658を備えている。通信事業者設備655と端末装置801とは、通信システム800を構成している。

【0133】端末装置801が通信への利用に供されるまでの処理の流れは、図11のフローチャートと同等に描かれる。ただし、ステップS205の内部フローは、図21のステップS260の処理へ置き換えられる。ステップS260の処理が開始されると、端末装置801は、識別符号Cdおよび記憶符号Coを通信事業者設備655へ送信する(S261)。それとともに、通信事業者設備655は、通信回路656によって識別符号Cdおよび記憶符号Coを受信する(S262)。

【0134】つぎに、通信事業者設備655は、判定回路657によって、識別符号Cdと記憶符号Coとを比較し、双方が互いに一致するか否かを判定し、判定結果を示す判定信号Enを通信回路656へ伝える(S263)。通信事業者設備655は、判定信号Enが符号の一致を示すときには(S264)、端末装置801の使用者が正当使用者であるとの認証を行い、判定信号Enが符号の不一致を示すときには(S264)、認証を行わない。通信事業者設備655は、例えば、認証を行うときには通信を許可して通信処理を続行し(S265)、認証を行わないときには、通信を不許可として、通信処理を中止する(S268)。

【0135】また、識別符号Cdおよび記憶符号Coを記録するよう指示がなされている場合には(S266)、認証を行わない場合に識別符号Cdおよび記憶符号Coが顧客データメモリ658へ記録される(S267)。そして、例えば通信処理が中止された(S278)後に、識別符号Cdおよび記憶符号Coを、過去に記録された顧客データメモリ658の内容と照合することにより(S269)、不正使用者の特定がなされる(S270)。

【0136】認証を行わないときに、通信処理を中止することなく、識別符号Cdおよび記憶符号Coの記録(S267)のみを行うことも可能である。さらに、識別符号Cdおよび記憶符号Coの記録(S267)を、認証結果とは無関係に実行することも可能である。後者の場合には、ステップS267の処理は、例えば、ステップS263とS264の間で実行される。

【0137】このように、図20の端末装置801では、識別符号Cdおよび記憶符号Coを通信事業者設備655の側で行われる認証処理の判断材料に供することができ、それにより、半導体基板の取り替えによる不正使用を認証の対象から排除して、精度の高い認証を実現することができる。

【0138】図22は、実施の形態4による端末装置の別の構成例を示すブロック図である。この端末装置801が備える半導体装置652は、比較回路403が除去

され、通信回路405aが識別符号Cd1、Cd2および記憶符号Co1、Co2を通信信号の一部として通信事業者設備655へ、単に送信する点において、図14に示した実施の形態1の半導体装置1012とは特徴的に異なっている。

【0139】図22の通信事業者設備655は、通信回路656に加えて、判定回路657および顧客データメモリ658を備えている。通信事業者設備655と端末装置811とは、通信システム810を構成している。

【0140】端末装置811が通信への利用に供されるまでの処理の流れは、図15のフローチャートと同等に描かれる。ただし、ステップS245の内部フローは、図23のステップS280の処理へ置き換えられる。ステップS280の処理が開始されると、端末装置811は、識別符号Cd1、Cd2および記憶符号Co1、Co2を通信事業者設備655へ送信する(S211)。それにともない、通信事業者設備655は、通信回路656によって識別符号Cd1、Cd2および記憶符号Co1、Co2を受信する(S272)。

【0141】つぎに、通信事業者設備655は、判定回路657によって、識別符号Cd1と記憶符号Co1とを比較し、双方が互いに一致するか否かを判定するとともに、識別符号Cd2と記憶符号Co2とを比較し、双方が互いに一致するか否かを判定する。そして、それらの判定結果を示す判定信号Enを通信回路656へ伝える(S273)。通信事業者設備655は、二つの比較の双方において符号の一致が認められたときには(S274)、端末装置811の使用者が正当使用者であるとの認証を行い、二つの比較のいずれかにおいて符号の不一致が認められたときには(S274)、認証を行わない。通信事業者設備655は、例えば、認証を行うときには通信を許可して通信処理を続行し(S275)、認証を行わないときには、通信を不許可として、通信処理を中止する(S278)。

【0142】また、識別符号Cd1、Cd2および記憶符号Co1、Co2を記録するよう指示がなされている場合には(S276)、認証を行わない場合に識別符号Cd1、Cd2および記憶符号Co1、Co2が顧客データメモリ658へ記録される(S277)。そして、例えば通信処理が中止された(S278)後に、識別符号Cd1、Cd2および記憶符号Co1、Co2を、過去に記録された顧客データメモリ658の内容と照合することにより(S279)、不正使用者の特定がなされる(S280)。

【0143】認証を行わないときに、通信処理を中止することなく、識別符号Cd1、Cd2および記憶符号Co1、Co2の記録(S277)のみを行うことも可能である。さらに、識別符号Cd1、Cd2および記憶符号Co1、Co2の記録(S277)を、認証結果とは無関係に実行することも可能である。後者の場合には、

ステップS277の処理は、例えば、ステップS273とS274の間で実行される。

【0144】このように、図23の端末装置811では、識別符号Cd1、Cd2および記憶符号Co1、Co2を通信事業者設備655の側で行われる認証処理の判断材料に供することができ、それにより、半導体基板の取り替えによる不正使用を認証の対象から排除して、精度の高い認証を実現することができる。また、二つの識別符号Cd1、Cd2が比較の対象とされるので、図21の端末装置801よりもさらに、認証の精度を高めることができる。

【0145】[5. 実施の形態5] 実施の形態5では、実施の形態1または2による半導体装置において、半導体基板の間での識別符号Cdおよび記憶符号Coのやりとりを、暗号化した形式で行う形態について説明する。

【0146】図24は、実施の形態5による半導体装置の構成を示すブロック図である。図24が示す半導体装置630では、符号生成部400が形成されている半導体基板CH20またはCH22に、暗号化回路631、復号化回路632および鍵生成部633が形成されている。

【0147】鍵生成部633は暗号化のための鍵Kを生成する。鍵Kは、識別符号Cdと同様に、半導体基板CH20またはCH22に固有の符号として生成される。暗号化回路631は、符号生成部400が生成する識別符号Cdを、鍵生成部633が生成する鍵Kにもとづいて識別符号Cd#へと暗号化し、半導体基板CH21に形成されたメモリ601へ送出する。メモリ601は、暗号化された識別符号Cd#を、暗号化された記憶符号Co#として記憶する。

【0148】復号化回路632は、メモリ601に記憶されている暗号化された記憶符号Co#を読み出し、鍵生成部633が生成する鍵Kにもとづいて記憶符号Coへと復号化し、比較回路403へ供給する。所定回路405は、比較回路403が出力する判定信号Enにもとづいて、動作または非動作となる回路部分を含んでいる。

【0149】以上のように、半導体装置630では、異なる半導体基板の間で、暗号化された形式で識別符号Cdおよび記憶符号Coがやりとりされるので、識別符号Cdおよび記憶符号Coのいずれをも外部から読み取ることができない。このため、不正使用に対する障壁がさらに高められる。

【0150】図25は、鍵生成部633の内部構成の一例を示すブロック図である。図25の例では、鍵生成部633は、OTPROM602を備えており、鍵Kは、半導体装置630の出荷時にOTPROM602に書き込まれる。このため、鍵生成部633が生成する鍵Kを不正に変更することができない。また、鍵Kが半導体装置630の出荷時にすでに書き込まれているので、鍵K

が使用者へ漏洩することがない。

【0151】図26は、鍵生成部633の内部構成の別の一例を示すブロック図である。図26の鍵生成部633は、図2に示した半導体素子401と符号化回路402とを備えている。符号化回路402は、半導体素子401の電気的特性をアナログ信号A<sub>n</sub>として読み出し、デジタル信号へ変換する。変換によって得られたデジタル信号は、鍵Kとして出力される。

【0152】半導体素子401の電気的特性として、半導体素子401の個体毎にばらつきを持った特性が選ばれる。それにより、鍵Kは、半導体素子401の個体毎にばらついた値として生成されるので、鍵生成部633が形成されている半導体基板に固有の識別符号としての性格を備えることとなる。鍵Kを書き込む必要もなく、さらに、量産される多数の半導体装置630の間で、同一工程で製造された半導体素子401を用いることができるので、半導体装置630の製造を簡略化することができる。また、鍵Kのもとになる半導体素子401の電気的特性を外部から変更することができないので、鍵Kの不正な変更に対する障壁が高いという利点も得られる。

【0153】図3～図6に例示したように、半導体装置401が多結晶体を備え、その結晶構造のばらつきに由来してばらつく電気的特性を利用することが可能である。多結晶体の結晶構造のばらつきは大きく、それに由来して電気的特性のばらつきも大きいので、鍵Kのばらつきの幅を広く確保することが可能である。すなわち、量産される多数の半導体装置630の間で、互いに鍵Kが一致しないようにすることが容易である。

【0154】図27は、図9の端末装置1001において、半導体装置1002の代わりに図24の半導体装置630を用い、所定回路405を通信回路405aとした場合に、端末装置1001が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置630が製造される（S301）。その最終工程、ないしそれ以前に、暗号化された識別符号C<sub>d</sub>#がメモリ601へ記憶符号C<sub>o</sub>#として記録される（S302）。その後、半導体装置630が電話機メーカーへ納入され、電話機メーカーによって端末装置1001が組み立てられる（S303）。完成した端末装置1001は、使用者へ供給された後（S304）、使用者による通信への利用に供される（S305）。

【0155】ステップS306～S310は、端末装置1001を用いた通信の手順、すなわちステップS305の内部フローを表している。通信が開始されると、端末装置1001は、記憶符号C<sub>o</sub>#をメモリ601から読み出す（S306）。つぎに、復号化回路632によって記憶符号C<sub>o</sub>#が記憶符号C<sub>o</sub>へと復号化されることにより、比較回路403によって、識別符号C<sub>d</sub>と記

憶符号C<sub>o</sub>との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号E<sub>n</sub>が生成される（S307）。

【0156】判定信号E<sub>n</sub>が符号の一致を示すときには（S308）、通信回路405aは通信機能を維持することにより、通信処理を続行する（S309）。一方、判定信号E<sub>n</sub>が符号の不一致を示すときには（S308）、通信回路405aは送信機能または受信機能の少なくとも一方を停止することにより、通信を不能にする（S310）。通信が完了すると、処理は終了する。

【0157】図28は、実施の形態5による半導体装置の別の構成例を示すブロック図である。図28が示す半導体装置635は、図13の半導体装置620において、識別符号C<sub>d</sub>1、C<sub>d</sub>2および記憶符号C<sub>o</sub>1、C<sub>o</sub>2が、二つの半導体基板の間で、暗号化した形式でやりとりされるように構成されている。すなわち、符号生成部400、比較回路403およびメモリ601が形成されている二つの半導体基板CH20（またはCH22）およびCH3の双方に、暗号化回路631、復号化回路632および鍵生成部633が形成されている。

【0158】半導体基板CH20（またはCH22）では、鍵生成部633は半導体基板CH20（またはCH22）に固有の鍵K1を生成し、暗号化回路631は識別符号C<sub>d</sub>1を鍵K1にもとづいて識別符号C<sub>d</sub>1#へと暗号化し、半導体基板CH23のメモリ601へ送出する。半導体基板CH23のメモリ601は、識別符号C<sub>d</sub>1#を記憶符号C<sub>o</sub>1#として記憶する。半導体基板CH20（またはCH22）の復号化回路632は、メモリ601から記憶符号C<sub>o</sub>1#を読み出し、鍵K1にもとづいて記憶符号C<sub>o</sub>1へと復号化して比較回路403へ供給する。

【0159】半導体基板CH23では、鍵生成部633は半導体基板CH23に固有の鍵K2を生成し、暗号化回路631は識別符号C<sub>d</sub>2を鍵K2にもとづいて識別符号C<sub>d</sub>2#へと暗号化し、半導体基板CH20（またはCH22）のメモリ601へ送出する。半導体基板CH20（またはCH22）のメモリ601は、識別符号C<sub>d</sub>2#を記憶符号C<sub>o</sub>2#として記憶する。半導体基板CH23の復号化回路632は、メモリ601から記憶符号C<sub>o</sub>2#を読み出し、鍵K2にもとづいて記憶符号C<sub>o</sub>2へと復号化して比較回路403へ供給する。所定回路405は、二つの比較回路403が出力する二つの判定信号E<sub>n</sub>1、E<sub>n</sub>2の組にもとづいて、動作または非動作となる回路部分を含んでいる。

【0160】以上のように、半導体装置635では、異なる半導体基板の間で、暗号化された形式で識別符号C<sub>d</sub>1、C<sub>d</sub>2および記憶符号C<sub>o</sub>1、C<sub>o</sub>2がやりとりされるので、識別符号C<sub>d</sub>1、C<sub>d</sub>2および記憶符号C<sub>o</sub>1、C<sub>o</sub>2のいずれをも外部から読み取ることができない。このため、不正使用に対する障壁がさらに高めら



れる。また、実施の形態 2 の半導体装置 620 (図 13) と同様に、二つの判定信号  $E_{n1}$ 、 $E_{n2}$  が用いられるので、半導体基板の取り替えによる不正使用に対する障壁をさらに高めることが可能となる。

【0161】また、符号生成部 400 が形成された半導体基板が 3 個以上である半導体装置においても、同様に、暗号化回路 631、復号化回路 632 および鍵生成部 633 を、各半導体基板に配置することによって、異なる半導体基板の間で識別符号および記憶符号を暗号化した形式でやりとりすることが可能である。

【0162】図 29 は、図 14 の端末装置 1011 において、半導体装置 1012 の代わりに図 28 の半導体装置 635 を用い、所定回路 405 を通信回路 405a とした場合に、端末装置 1011 が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置 635 が製造される (S341)。その最終工程、ないしそれ以前に、各半導体基板の暗号化された識別符号  $Cd1\#$ 、 $Cd2\#$  が、他方の半導体基板のメモリ 601 へ記憶符号  $Co1\#$ 、 $Co2\#$  として記録される (S342)。その後、半導体装置 620 が電話機メーカへ納入され、電話機メーカによって端末装置 1011 が組み立てられる (S343)。完成した端末装置 1011 は、使用者へ供給された後 (S344)、使用者による通信への利用に供される (S345)。

【0163】ステップ S346~S350 は、端末装置 1011 を用いた通信の手順、すなわちステップ S345 の内部フローを表している。通信が開始されると、端末装置 1011 は、記憶符号  $Co1\#$  および  $Co2\#$  を二つのメモリ 601 から読み出す (S346)。つぎに、二つの復号化回路 632 によって記憶符号  $Co1\#$ 、 $Co2\#$  が記憶符号  $Co1$ 、 $Co2$  へと復号化された後、一方の比較回路 403 によって、識別符号  $Cd1$  と記憶符号  $Co1$  との比較が行われ、双方が一致するかどうかに関する判定結果を表現する判定信号  $E_{n1}$  が出力されると同時に、他方の比較回路 403 によって、識別符号  $Cd2$  と記憶符号  $Co2$  との比較が行われ、双方が一致するかどうかに関する判定結果を表現する判定信号  $E_{n2}$  が出力される (S347)。

【0164】判定信号  $E_{n1}$ 、 $E_{n2}$  のいずれもが、符号の一致を示すときには (S348)、通信回路 405a は通信機能を維持することにより、通信処理を続行する (S349)。一方、判定信号  $E_{n1}$ 、 $E_{n2}$  のいずれかが、符号の不一致を示すときには (S348)、通信回路 405a は送信機能または受信機能の少なくとも一方を停止することにより、通信を不能にする (S350)。通信が完了すると、処理は終了する。

【0165】〔6. 実施の形態 6〕実施の形態 6 では、実施の形態 5 による半導体装置において、暗号化された識別符号の送出と、暗号化された記憶符号の入力とを、

排他的に行うスイッチ回路が設けられる形態について説明する。

【0166】図 30 は、実施の形態 6 による半導体装置の構成を示すブロック図である。図 30 が示す半導体装置 640 では、符号生成部 400 が形成されている半導体基板  $CH40$  または  $CH42$  に、暗号化回路 631、復号化回路 632 および鍵生成部 633 に加えて、スイッチ回路 641 が形成されている。スイッチ回路 641 は、暗号化回路 631 から半導体基板  $CH41$  に形成されたメモリ 601 へ送出される識別符号  $Cd\#$  の伝達経路、およびメモリ 601 から復号化回路 632 へ送られる記憶符号  $Co\#$  の伝達経路に介挿されており、識別符号  $Cd\#$  の伝達と記憶符号  $Co\#$  の伝達とを排他的に行う。

【0167】使用者が不正使用を意図して、暗号化回路 631 が出力する識別符号  $Cd\#$  が復号化回路 632 へそのまま入力されるように、半導体基板  $CH40$  (または  $CH42$ ) の端子を短絡したとしても、スイッチ回路 641 の働きにより、識別符号  $Cd\#$  が復号化回路 632 へそのまま入力されることはない。すなわち、端子の短絡によって不正使用が意図されても、識別符号  $Cd$  と記憶符号  $Co$  とが一致しているかのように比較回路 403 に見せかけることはできない。このように、半導体装置 640 は、半導体基板の端子を短絡することによってなされる応用機器の不正使用をも防止する。

【0168】スイッチ回路 641 は、符号生成部 400 と暗号化回路 631 との間、および比較回路 403 と復号化回路 632 との間に介挿しても、図 30 の半導体装置 640 と同等の効果が得られる。一般に、スイッチ回路 641 は、符号生成部 400 からメモリ 601 へ至る識別符号  $Cd$  (または  $Cd\#$ ) の伝達経路、および、メモリ 601 から比較回路 403 へ至る記憶符号  $Co$  (または  $Co\#$ ) の伝達経路に介挿されておればよい。

【0169】また、スイッチ回路 641 は、暗号化回路 631 等を備えない図 1 の半導体装置 600 にも適用可能である。すなわち、図 1 の半導体装置 600 において、符号生成部 400 からメモリ 601 へ至る識別符号  $Cd$  の伝達経路、およびメモリ 601 から比較回路 403 へ至る記憶符号  $Co$  の伝達経路に介挿されるように、半導体基板  $CH1$  (または  $CH3$ ) にスイッチ回路 641 を形成することも可能である。それにより、図 30 の半導体装置 640 と同等の効果が得られる。

【0170】さらに、スイッチ回路 641 は、図 13 に示した半導体装置 620、および図 28 に示した半導体装置 635 に適用することも可能である。図 13 の半導体装置 620 に適用される場合には、スイッチ回路 641 は、半導体基板  $CH4$  (または  $CH6$ ) と半導体基板  $CH5$  の双方に形成される。図 28 の半導体装置 635 に適用される場合には、スイッチ回路 641 は、半導体基板  $CH20$  (または  $CH22$ ) と半導体基板  $CH23$



の双方に形成される。

【0171】 [7. 実施の形態7] 実施の形態5で説明した半導体素子401を備える鍵生成部633は、ホストコンピュータとデータのやり取りを行う一般の端末装置にも応用可能である。実施の形態7では、そのように構成された端末装置について説明する。

【0172】 図31は、実施の形態7による端末装置の構成を示すブロック図である。端末装置821とこれに接続されるホストコンピュータ825とは、互いにデータDdをやり取りするシステム820を構成している。端末装置821は、データDdを入力するデータ入力部822、およびデータDdを出力するデータ出力部823に加えて、暗号化回路631、復号化回路632および鍵生成部633を備えている。鍵生成部633は暗号化のための鍵Kを生成する。暗号化回路631は、データ入力部822から入力されたデータDdを、鍵生成部633が生成する鍵KにもとづいてデータDd#へと暗号化し、ホストコンピュータ825へ送出する。

【0173】 ホストコンピュータ825は、暗号化されたデータDd#をデータDo#としてメモリ826へ記憶する。復号化回路632は、メモリ826に記憶されている暗号化されたデータDo#を受信すると、鍵生成部633が生成する鍵KにもとづいてデータDoへと復号化し、データ出力部823へ伝える。データDoはデータDdと同一である。このように、端末装置821では、ホストコンピュータ825との間で、暗号化した形式でデータがやりとりされるので、データが表現する情報の漏洩に対する障壁が高い。

【0174】 鍵生成部633の内部構成は、図26で示される。すなわち、鍵生成部633は、半導体素子401の個体毎にばらつく電気的特性を利用して、端末装置に固有の鍵Kを生成する。したがって、端末装置821の製造工程で、鍵Kを書き込む必要もなく、さらに、量産される多数の端末装置821の間で、同一工程で製造された半導体素子401を用いることができるので、端末装置821の製造を簡略化することができる。また、鍵Kのもとになる半導体素子401の電気的特性を外部から変更することができないので、鍵Kの不正な変更に対する障壁が高いという利点も得られる。

【0175】 図32は、実施の形態7による端末装置の別の構成例を示すブロック図である。図32の端末装置は、本体部828に脱着自在のICカード829に鍵生成部633が組み込まれている点において、図31の端末装置821とは特徴的に異なっている。ICカード829が本体部828に装着されることにより、本体部828に設けられた暗号化回路631および復号化回路632が、鍵生成部633に接続される。

【0176】 本体部828に脱着自在のICカード829に鍵生成部633が組み込まれているので、携帯に便利なICカード829を自在に持ち運ぶことにより、離

れた場所に設置された複数の本体部821に対して、同一の鍵Kを使用することが可能である。

【0177】 [8. 実施の形態8] 実施の形態8では、実施の形態4による端末装置801において、記憶符号Coを記憶するメモリ654が、本体部に脱着自在の補助部に組み込まれている形態について説明する。

【0178】 図33は、実施の形態8による端末装置の構成を示すブロック図である。この端末装置は、本体部651と、補助部としての充電器653とに分離されており、図20の端末装置801において、半導体基板CH50を本体部651へ組み込み、半導体基板CH51を充電器653へ組み込んだ装置と同等である。本体部651には図示しない充電可能な電池が備わっており、充電器653は、本体部651へ装着されたときに電池を充電する。

【0179】 充電器653が本体部651へ装着されたときには、電池が充電されるだけでなく、半導体基板CH50を有する半導体装置652と半導体基板CH51との間が接続される。通信回路405aは、充電器653が本体部651へ装着されないときには、識別符号Cdと記憶符号Coの中で、識別符号Cdのみを通信事業者設備655へ送信し、充電器653が本体部651へ装着されているときには、識別符号Cdと記憶符号Coの双方を送信する。通信事業者設備655、端末装置本体部651および充電器653は、通信システム650を構成する。

【0180】 図34は、図33の端末装置が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置652が製造され(S501)、その後、半導体装置652が電話機メーカーへ納入され、電話機メーカーによって端末装置本体部651が組み立てられる(S502)。これと並行ないし前後して、部品としてのメモリ654が製造され(S503)、その後、電話機メーカーによって充電器653が組み立てられる(S504)。

【0181】 端末装置本体部651と充電器653の双方が完成すると、識別符号Cdが記憶符号Coとしてメモリ654へ記録され(S505)、端末装置本体部651と充電器653のセットが、通信事業者設備655を保有する通信事業者へ納入される(S506)。ステップS501～S506までのいずれかの段階で、識別符号Cdと記憶符号Coの双方が読み取られ、通信事業者設備655の顧客データメモリ658へ登録される(S507)。その後、端末装置本体部651および充電器653のセットが、使用者へ供給された後(S508)、使用者による通信への利用に供される(S509)。

【0182】 図35および図36は、ステップS509の内部手順を示すフローチャートである。通信が開始されると、端末装置の使用が非充電時の使用である場合、

すなわち充電器653が本体部651に装着されていない場合には(S520)、端末装置本体部651は、識別符号Cdを通信事業者設備655へ送信する(S521)。それにもない、通信事業者設備655は、通信回路656によって識別符号Cdを受信する(S522)。

【0183】つぎに、通信事業者設備655は、判定回路657によって、識別符号Cdと登録された識別符号Cdとを比較し、双方が互いに一致するか否かを判定し、判定結果を示す判定信号Enを通信回路656へ伝える(S523)。通信事業者設備655は、判定信号Enが符号の一致を示すときには(S524)、端末装置本体部651の使用者が正当使用者であるとの認証を行い、判定信号Enが符号の不一致を示すときには(S524)、認証を行わない。通信事業者設備655は、例えば、認証を行うときには通信を許可して通信処理を続行し(S525)、認証を行わないときには、通信を不許可として、通信処理を中止する(S526)。

【0184】端末装置の使用が充電時の使用である場合、すなわち本体部651が充電器653に接続された状態で通信に使用されている場合には(S520、S530)、端末装置本体部651は、識別符号Cdと記憶符号Coの双方を通信事業者設備655へ送信する(S531)。それにもない、通信事業者設備655は、通信回路656によって識別符号Cdおよび記憶符号Coを受信する(S532)。

【0185】つぎに、通信事業者設備655は、判定回路657によって、識別符号Cdと登録された識別符号Cdとを比較し、双方が互いに一致するか否かを判定するとともに、記憶符号Coと登録された記憶符号Coとを比較し、双方が互いに一致するか否かを判定する。判定回路657は、二つの判定結果を表現する判定信号Enを通信回路656へ伝える(S533)。

【0186】通信事業者設備655は、判定信号Enにもとづいて、いずれの判定においても符号の一致が認められるときには(S534)、端末装置の使用者が正当使用者であるとの認証を行い、いずれかの判定において符号の不一致が認められるときには(S534)、認証を行わない。ステップS533では、二つの符号Cd、Coの双方にもとづいて判定がなされるので、符号CdのみにもとづいてステップS523での判定に比べて、判定の確度が高い。すなわち、ステップS533の判定にもとづいてなされる認証は、ステップS523の判定にもとづいてなされる認証に比べて、端末装置が正当に使用されていることをより高い確度で証明する高位の(高レベルの)認証に相当する。

【0187】したがって、通信事業者設備655は、レベルの異なる二つの認証を、手続の重要性に応じて使い分けることが可能となる。一例として、通信事業者設備655は、ステップS533の判定にもとづいて認証を

行うときには、端末装置が通信に使用されているときに(S535)通信を許可して通信処理を続行する(S536)だけでなく、通信に使用されているか否かに関わりなく、それ以前の通信(前回にステップS533の判定にもとづいて認証されてから今回までの通信)に対する通信料金を、裏付けられたものとして記録する(S537)。これにより、端末装置の紛失を装って料金支払いの義務を逃れる違法行為を防止することが可能となる。端末装置本体部651と充電器653との双方を同時に紛失するというケースは希少であるため、裏付けは十分に高い確度を持ったものとなる。

【0188】また、通信事業者設備655は、ステップS533の判定にもとづいて認証を行わないときには、すでに登録されている識別符号Cdおよび記憶符号Coとは別個に、ステップS532で受信した識別符号Cdおよび記憶符号Coを、顧客データメモリ658へ記録する。記録された識別符号Cdおよび記憶符号Coは、不正使用者の特定に役立てることができる。

【0189】図34に戻って、ステップS507では、識別符号Cdと記憶符号Coの双方が登録される代わりに、識別符号Cdのみが登録されても良い。この場合には、ステップS501～S506までのいずれかの段階で、識別符号Cdのみが読み取られれば足りる。記憶符号Coの登録は、使用者がはじめて行う充電時の使用(S530)の際に、ステップS531で送信される記憶符号Coを、顧客データメモリ658へ登録することにより達成される。

【0190】なお、メモリ601は、充電器653だけでなく、本体部に脱着自在の何らかの補助部に組み込まれても良い。ただし、補助部が充電器653である図33の形態では、使用者に特別の手間を要求することなく、本体部651と補助部との結合が定期的に行われるという利点が得られる。

【0191】[9. 実施の形態9] 実施の形態9では、実施の形態8による端末装置において、本体部と補助部の間、および本体部と通信事業者設備の間において、暗号化された形式で符号が伝送される形態について説明する。

【0192】図37は、実施の形態9による端末装置の構成を示すブロック図である。この端末装置は、本体部671が備える半導体装置672に、暗号化回路631および鍵生成部633が設けられており、充電器653にも暗号化回路631および鍵生成部676が設けられている点において、図33の端末装置とは特徴的に異なる。それにもない、通信事業者設備675には、復号化回路632が設けられている。通信事業者設備675、端末装置本体部671および充電器673は、通信システム670を構成する。

【0193】充電器673では、鍵生成部676は暗号化のための鍵K2を生成し、暗号化回路631はメモリ

601から読み出した記憶符号C oを鍵K 2にもとづいて暗号化し、記憶符号C o #として本体部671へ送出する。本体部671では、鍵生成部633は暗号化のための鍵K 1を生成し、暗号化回路631は符号生成部400が生成する識別符号C dを鍵K 1にもとづいて暗号化し、識別符号C d #として通信回路405aへ伝える。本体部671の暗号化回路631は、充電器673から送られる記憶符号C o #をも、鍵K 1にもとづいて暗号化し、記憶符号C o # #として通信回路405aへ伝える。記憶符号C o # #は、二つの鍵K 1, K 2によ

って二重に暗号化されている。  
【0194】通信回路405aは、暗号化された識別符号C d #および記憶符号C o # #を、通信事業者設備655へ送信する。通信事業者設備655は、復号化回路632によって識別符号C d #および記憶符号C o # #を、それぞれ識別符号C dおよび記憶符号C o #へと復号化し、判定回路657での判定の材料に供する。

【0195】このように、図37の端末装置では、本体部671と充電器673の間、および本体部671と通信事業者設備675の間において、暗号化された形式で符号が伝送されるので、これらの符号の漏洩に対する障壁が高いという利点が得られる。

【0196】本体部671において、好ましくは、鍵生成部633と暗号化回路631とは符号生成部400とともに、単一の半導体基板CH50（またはCH70）に形成される。それによって、鍵K 1および識別符号C dの漏洩に対する障壁がさらに高められる。同様に、充電器673において、鍵生成部676と暗号化回路631とは、メモリ601とともに、単一の半導体基板CH71に形成される。それによって、鍵K 2および記憶符号C oの漏洩に対する障壁がさらに高められる。

【0197】図38は、図37の端末装置が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置672が製造され（S701）、その後、半導体装置672が電話機メーカーへ納入され、電話機メーカーによって端末装置本体部671が組み立てられる（S702）。これと並行ないし前後して、部品としてのメモリ654が製造され（S703）、その後、電話機メーカーによって充電器673が組み立てられる（S704）。

【0198】端末装置本体部671と充電器673の双方が完成すると、識別符号C dが記憶符号C oとしてメモリ654へ記録され（S705）、端末装置本体部671と充電器673のセットが、通信事業者設備675を保有する通信事業者へ納入される（S706）。ステップS701～S706までのいずれかの段階で、識別符号C d、記憶符号C o #および鍵K 1が読み取られ、通信事業者設備675の顧客データメモリ658へ登録される（S707）。その後、端末装置本体部671および充電器673のセットが、使用者へ供給された後

（S708）、使用者による通信への利用に供される（S709）。

【0199】図39および図40は、ステップS709の内部手順を示すフローチャートである。通信が開始されると、端末装置の使用が非充電時の使用である場合、すなわち充電器673が本体部671に装着されていない場合には（S720）、端末装置本体部671は、識別符号C d #を通信事業者設備675へ送信する（S721）。それにともない、通信事業者設備675は、通信回路656によって識別符号C d #を受信する（S722）。

【0200】つぎに、通信事業者設備675は、復号化回路632によって、識別符号C d #を識別符号C dへと復号化した後、判定回路657によって、識別符号C dと登録された識別符号C dとを比較し、双方が互いに一致するか否かを判定する。そして、判定回路657は、判定結果を示す判定信号E nを通信回路656へ伝える（S723）。通信事業者設備675は、判定信号E nが符号の一致を示すときには（S724）、端末装置本体部671の使用者が正当使用者であるとの認証を行い、判定信号E nが符号の不一致を示すときには（S724）、認証を行わない。通信事業者設備675は、例えば、認証を行うときには通信を許可して通信処理を続行し（S725）、認証を行わないときには、通信を不許可として、通信処理を中止する（S726）。

【0201】端末装置の使用が充電時の使用である場合、すなわち本体部671が充電器673に接続された状態で通信に使用されている場合には（S720、S730）、端末装置本体部671は、識別符号C d #と記憶符号C o # #の双方を通信事業者設備675へ送信する（S731）。それにともない、通信事業者設備675は、通信回路656によって識別符号C d #および記憶符号C o # #を受信する（S732）。

【0202】つぎに、通信事業者設備675は、復号化回路632によって、識別符号C d #を識別符号C dへと復号化するとともに、記憶符号C o # #を記憶符号C o #へと復号化する。その後、通信事業者設備675は、判定回路657によって、識別符号C dと登録された識別符号C dとを比較し、双方が互いに一致するか否かを判定するとともに、記憶符号C o #と登録された記憶符号C o #とを比較し、双方が互いに一致するか否かを判定する。判定回路657は、二つの判定結果を表現する判定信号E nを通信回路656へ伝える（S733）。

【0203】通信事業者設備675は、判定信号E nにもとづいて、いずれの判定においても符号の一致が認められるときには（S734）、端末装置の使用者が正当使用者であるとの認証を行い、いずれかの判定において符号の不一致が認められるときには（S734）、認証を行わない。ステップS733の判定にもとづいてなさ

れる認証は、ステップS723の判定にもとづいてなされる認証に比べて、端末装置が正当に使用されていることをより高い確度で証明する高位の（高レベルの）認証に相当する。

【0204】一例として、通信事業者設備675は、ステップS733の判定にもとづいて高位の認証を行うときには、端末装置が通信に使用されているときに（S735）通信を許可して通信処理を続行する（S736）だけでなく、通信に使用されているか否かに関わりなく、それ以前の通信（前回にステップS733の判定にもとづいて認証されてから今回までの通信）に対する通信料金を、裏付けられたものとして記録する（S737）。また、通信事業者設備675は、ステップS733の判定にもとづいて高位の認証を行わないときには、すでに登録されている識別符号Cdおよび記憶符号Coとは別個に、ステップS732で受信した識別符号Cdおよび記憶符号Coを、顧客データメモリ658へ記録する。

【0205】図38に戻って、ステップS707では、識別符号Cd、記憶符号Coおよび鍵K1が登録される代わりに、識別符号Cdと鍵K1のみが登録されても良い。この場合には、ステップS701～S706までのいずれかの段階で、識別符号Cdのみが読み取られれば足りる。記憶符号Coの登録は、使用者がはじめて行う充電時の使用（S730）の際に、ステップS731で送信される記憶符号Coを、顧客データメモリ658へ登録することにより達成される。

【0206】以上のように、図37の端末装置を用いることにより、図33の端末装置を用いた場合と同様に、通信事業者設備675は、確度の異なる2段階の認証を、手続の重要性に応じて使い分けることができる。しかも、暗号化された形式で、識別符号Cdおよび記憶符号Coが送信されるので、これらの符号の漏洩に対する障壁が高い。

【0207】充電器673を紛失したり、あるいは故障を生じるなどにより、充電器673を交換することが必要な場合が想定される。このような場合に、すでに登録されている記憶符号Coを、あらたな充電器673に固有の記憶符号Coへと更新することができれば、正当使用者にとって都合がよい。それには、図41が示すように、図40の処理手順にステップS741およびS742を付加するとよい。図41の処理手順では、記憶符号Coの変更を行わないときには（S741）、図41と同様にステップS731～S738の処理が行われ、記憶符号Coの変更を行おうときには（S741）、登録された記憶符号Coを変更する処理が実行される（S742）。

【0208】図42および図43は、変更処理（S742）の内部手順を示すフローチャートである。変更処理が開始されると、端末装置から通信事業者設備675

へ、識別符号Cd#、記憶符号Co##、および端末識別番号とともに、登録された記憶符号Co#の変更の意志を表現する要求信号が送信される（S752）。それにともない、通信事業者設備675は、これらの符号、端末識別番号および信号を通信回路656によって受信する（S753）。

【0209】つぎに、通信事業者設備675は、復号化回路632によって、識別符号Cd#を識別符号Cdへと復号化するとともに、記憶符号Co##を記憶符号Co#へと復号化する。その後、通信事業者設備675は、判定回路657によって、識別符号Cdと登録された識別符号Cdとを比較し、双方が互いに一致するか否かを判定するとともに、記憶符号Co#と登録された記憶符号Co#とを比較し、双方が互いに一致するか否かを判定する。判定回路657は、二つの判定結果を表現する判定信号Enを通信回路656へ伝える（S753）。

【0210】通信事業者設備675は、判定信号Enにもとづいて、いずれの判定においても符号の一致が認められるときには（S754）、登録された記憶符号Co#の変更を許可する旨の通知を端末装置へ送信するとともに、新しい記憶符号Co#を持つ充電器673への交換を促すメッセージを、端末装置へ送信し表示させる。それに応じて、端末装置の使用者が、記憶符号Co#を有する充電器673を、新たな記憶符号Co#（便宜上、CoNew#と記載する）を有する充電器673へと交換すると（S757）、端末装置から通信事業者設備675へ、識別符号Cd#および記憶符号CoNew##が送信される（S758）。それにともない、通信事業者設備675は、これらの識別符号Cd#および記憶符号CoNew##を通信回路656によって受信する（S753）。

【0211】つぎに、通信事業者設備675は、復号化回路632によって、識別符号Cd#を識別符号Cdへと復号化するとともに、記憶符号CoNew##を記憶符号CoNew#へと復号化する（S760）。その後、通信事業者設備675は、顧客データメモリ658へ登録されている記憶符号Co#を、記憶符号CoNew#で更新する。

【0212】通信事業者設備675は、判定信号Enにもとづいて、いずれかの判定において符号の不一致が認められるときには（S754）、変更処理をそれ以上進めることなく、現在使用中の充電器673をそのまま使用して再度の操作を行うよう促すメッセージを、端末装置へ送信し表示させる（S755）。

【0213】ステップS742と同様の変更処理は、図40の処理手順だけでなく、暗号を用いない図36の処理手順にも、付加することが可能である。それにより、使用者は、図33の充電器653を交換することが可能となる。

【0214】充電器653、673が備えるメモリ654にOTPROMを用いる代わりに、書き換え可能なメモリ、例えばフラッシュROMを用いてもよい。上記した変更処理S742は、このような記憶符号C○#の書き換えが可能な充電器653、673の使用にも適している。不正な変更に対するセキュリティを高めるために、登録された記憶符号C○#の書き換えを、クレジットカード番号など課金を保証できる情報を端末装置が送信した場合に限定することも可能である。

【0215】図44および図45は、図38の通信処理(S709)の別の内部フローを示すフローチャートである。この通信処理(S770)では、認証が商取引へ利用される。すなわち、通信事業者設備675は、ステップS733の判定にもとづいて高位の認証を行うときには(S734)、端末装置が通信に使用されているときに(S735)、通信処理を継続して商取引を許可する(S736)とともに、端末装置が通信に使用されているか否かに関わりなく、それ以前の通信(前回にステップS733の判定にもとづいて認証されてから今回までの通信)においてなされた商取引が成立したものと記録する(S775)。一方、通信事業者設備675は、ステップS733の判定にもとづいて高位の認証を行わないときには、それ以前の通信においてなされた商取引が成立しなかったものとして記録する(S776)。

【0216】確度の高い認証にもとづいて商取引が成立した旨の記録がなされておれば、取引相手は当該記録にもとづいて、商取引は有効なものとして商品の発送等の様々な手続を進めることが可能であり、商取引が成立しなかった旨の記録があれば、商取引にもとづく手続を中止することができる。これにより、端末装置の不正使用にもとづく不正な商取引による損害を解消ないし低減することができる。

【0217】さらに望ましくは、通信事業者設備675は、ステップS733の判定にもとづいて高位の認証を行わないときには、非充電時の商取引をも不可とするための記録を行う(S777)。記録は、例えば、通信事業者設備675が備えるコンピュータシステムのレジスタに、フラグを立てることによって行われる。

【0218】端末装置の使用が非充電時の使用である場合、すなわち充電器673が本体部671に装着されていない場合に(S720)、ステップS723の判定にもとづいて認証をおこなうときには、非充電時の商取引を不可とする記録がなされているか否か(例えば、上記したフラグが立っているか否か)が判定される(S771)。そして、通信事業者設備675は、上記した記録がなされていないければ、通信処理を継続して商取引を許可し(S772)、記録がなされておれば、通信処理を中止する(S773)。

【0219】このように、充電器673が本体部671

に装着されない状態でなされる通常の認証に、過去になされた確度の高い判定結果が反映されるので、商取引などの重要な手続を、通常の認証の下で行うことができる。なお、図35および図36に示したステップS509においても、図44および図45に示したステップS772~S773、S774~S777を実行することが可能である。

【0220】図37の充電器673は、携帯に便利なICカードに置き換えることも可能である。この場合には、使用者がICカードを時折、本体部671へ装着する必要があるが、ICカードから本体部671への記憶符号C○#の伝送を、無線を媒体として行うことが可能であれば、使用者が意識的にICカードを本体部671へ装着する手間を省くことができ、使用者に便利である。図46はそのように構成された端末装置を例示するブロック図である。

【0221】図46の端末装置は、本体部691が備える半導体装置692に、通信インタフェース694が設けられており、ICカード693にも通信インタフェース695が設けられている。通信インタフェース694は、例えば、鍵生成部633、暗号化回路631および符号生成部400とともに、単一の半導体基板CH90(またはCH91)に形成される。同様に、通信インタフェース695は、例えば、鍵生成部676、暗号化回路631およびメモリ601とともに、単一の半導体基板CH92に形成される。

【0222】通信インタフェース694、695は、無線通信を行うインタフェースであり、例えば、Bluetooth規格に準拠している。したがって、ICカード693から本体部691への記憶符号C○#の伝送は、無線を媒介して行われる。このため、例えば、ICカード693が使用者の着衣のポケットの中に投入されており、本体部691が使用者が携帯する鞆の中に収納されていても、通信事業者設備675へ、識別符号Cd#と記憶符号C○#の双方を送信することが可能となる。ICカード693の代わりに、携帯電話機としての本体部に差し込んで使用されるUIM(Universal subscriber Identification Module)のようなカードを用いてもよい。ただし、その場合には、使用者が本体部とカードとを同時に紛失する可能性が無視できないので、図46が示すように、別個の独立した機器との間で記憶符号C○#をやり取りする形態がより望ましい。

【0223】なお、通信システム670において、図12が示すように、通信事業者設備655は、銀行のATMシステムなど、他の事業者設備に置き換えが可能である。例えば、認証にもとづいて商取引を行う場合には、認証および商取引の許可、不許可等の処理を、端末装置の取引相手である銀行のATMシステムが直接に行うことも可能である。他の実施の形態における通信システムにおいても同様である。



【0224】[10. 実施の形態10] 従来においては、地下街あるいはビルディングの中など、電波が侵入し難い領域では、端末装置は通信事業者設備を媒介した無線通信を行い得ないという問題点があった。あるいは、そのような領域において無線通信を可能にするためには、多くの基地局を設ける必要があった。実施の形態10では、通信事業者設備を媒介した無線通信を行い得ない領域においても、基地局なしで無線通信を可能にする端末装置および通信方法について説明する。本実施の形態による端末装置および通信方法においては、実施の形態5などで示した暗号化回路、復号化回路および鍵生成部が有用な役割を果たす。

【0225】[10.1. 概略] 図47は、本実施の形態による通信方法を示す説明図である。この方法では、通信事業者設備を媒介した無線通信と、通信事業者設備を媒介しない無線通信網の形成が可能な端末装置が用いられる。以下に説明する例では、上記無線通信網として、無線LANが採用される。電波が侵入し難い領域においても、通常時には群衆が集合ないし通行している。現在においては、これらの群衆の少なからぬ部分が携帯電話機を携帯している。これら群衆が携帯する携帯電話機が、上記した機能を有する端末装置であれば、図47が示すように、複数の端末装置840a～840dの間で無線LANを形成することにより、互いに通信を行うことが可能となる。例えば、端末装置840aと端末装置840dとが、端末装置840b、840cを中継することにより、互いに通信を行うことが可能となる。

【0226】無線LANとして、例えばBluetooth規格に準拠したものを用いることができる。この場合には、一つの端末装置は、自身を中心とする半径10m以内にある他の端末装置と、無線を媒介して通信を行うことが可能である。地下街、あるいはビルディングの中には、通常時には10m以内に多数の通行者、作業員等が存在しており、これらの人々が携帯する端末装置を経由することによって、地下街、あるいはビルディング内の全体をカバーする通信が可能となる。

【0227】無線LANを利用することにより、小さい電力で運営できるという利点も得られる。例えば10mを到達範囲とする無線LANでは、1kmを到達範囲とする無線通信に比べて、電波を発射するのに要する消費電力は $(1/100)^2$ 倍である。1km離れた端末装置の間で通信を行うために、平均1m間隔で並んだ1000個の端末装置が通信を中継したとしても、全消費電力は、 $(1/100)^2 \times 1000 = 1/10$ 倍に低減される。

【0228】また、地下街、あるいはビルディング内のような電波が侵入し難い領域だけでなく、一般に多数の人々が集合、通行ないし居住する空間の中で、無線LANを形成することにより、上記空間の全体で端末装置どうしを媒介した通信が実現する。当該空間の中に地下

街、あるいはビルディング内のような電波が侵入し難い領域があっても、端末装置どうしを媒介した通信が阻害されることがない。また、各家庭内の端末装置が無線LANを中継することにより、地上の住宅街においても、ほとんど基地局のいない低消費電力の無線通信システムを構築することができる。

【0229】[10.2. 端末装置の例] 図47が示す無線LANを媒介した通信では、不特定多数の人が携帯する端末装置を経由して通信が行われるために、通信内容の漏洩に対するセキュリティを確保する必要がある。それには図48が示すように、通信事業者設備を媒介した無線通信を行う部分（遠距離通信部と仮称する）847と、無線LANを媒介した通信を行う部分（近距離通信部と仮称する）848とが、電気的に分離されるように端末装置840を構成するとよい。

【0230】遠距離通信部847は、通信事業者設備を媒介した無線通信を行う通信回路841、音声を入力するためのマイク842、音声を出力するためのスピーカ843、ダイヤル番号などをキー操作等により入力するための入力部845、および文字、記号、図形等により情報を表示する表示パネル844を備えている。近距離通信部848は、無線LANを形成することにより無線通信を行う無線LAN回路846を備えている。図48の端末装置840では、遠距離通信部847と近距離通信部848とが、互いに分離されているので、端末装置840を所持する使用者自身は、無線LANを媒介した通信を行うことはできず、単に他人の通信を中継する役割を担うに過ぎない。

【0231】端末装置の所持者自身が無線LANを媒介した通信を行うことを可能にし、しかも通信内容の漏洩に対するセキュリティを確保するには、図49が示すように、暗号技術を用いるとよい。通信事業者設備を媒介とした無線通信で暗号技術が用いられる場合であっても、それとは異なる独自の暗号体系が、無線LANを媒介とした通信に用いられる。

【0232】無線LAN回路846と通信回路841の間には、通信信号の伝達経路が設けられており、この伝達経路には、切替回路856、暗号化回路851および復号化回路852が介挿されている。切替回路856は、上記伝達経路の接続と切断とを選択自在に実行する。切替回路856が上記伝達経路を接続するときには、端末装置850の使用者と他者との間で、無線LANを媒介した通信が実現する。切替回路856が上記伝達経路を切断するときには、端末装置850は無線LANを媒介した他者どうしの通信を単に中継するに過ぎない。なお、図49では、便宜上、アンテナが送信用と受信用とに分けて描かれるが、これらは通常においては単一のアンテナに共通化されている。

【0233】暗号化回路851、復号化回路852および鍵生成部853は、端末装置850の使用者と他者と



の間で無線 LAN を媒介した通信を行うために、切替回路 856 が上記伝達経路を接続するときに、その機能を果たす。鍵生成部 853 は、暗号化のための鍵 K を生成する。暗号化回路 851 は、通信回路 841 から無線 LAN 回路 846 の送信回路 855 へ送られる送信信号を、鍵 K にもとづいて暗号化する。復号化回路 852 は、無線 LAN 回路 846 の受信回路 854 から通信回路 841 へ送られる受信信号を鍵 K にもとづいて復号化する。

【0234】ここで、鍵 K は無線 LAN を媒介して端末装置 850 が通信を行う通信相手と共通の鍵である必要がある。そのために、鍵生成部 853 は図 50 が示す内部構成を有する。すなわち、鍵生成部 853 は、符号生成部 633 および鍵演算部 857 を備えている。符号生成部 633 は、端末装置 850 に固有な識別符号 C d を生成する。鍵演算部 857 は、無線 LAN 回路 846 を通じて通信相手から送られる別の符号とにもとづいて、端末装置 850 の使用者と通信相手との間で共通に使用可能な共通鍵を算出し、鍵 K として出力する。

【0235】符号生成部 633 は、実施の形態 5 の図 25 または図 26 に示す形態を採ることが望ましい。それにより、実施の形態 5 と同様の効果が得られる。図 50 は、符号生成部 633 が図 26 と同等に形成された例を示している。

【0236】[10.3. 鍵生成の手順] 図 51 は、鍵生成部 853 が鍵 K を生成する手順の一例を示すフローチャートである。図 51 の手順は、周知の DH 法を利用している。端末装置 850 と他の端末装置との間で、無線 LAN を媒介した通信が開始されると、他の端末装置すなわち通信相手が新規であるか否かが判定される (S801)。通信相手が新規であれば、あらかじめ定められた素数  $p$  と、あらかじめ定められた自然数  $g$  とにもとづいて、鍵演算部 857 によって、符号  $\alpha \# = g \alpha \bmod (p)$  が算出される (S802)。ここで、 $\alpha$  は符号生成部 633 が生成する識別符号 C d である。また、 $\bmod ()$  は、整数論におけるモードを表す。素数  $p$  および自然数  $g$  は、すべての端末装置の間で共通であり、公開鍵に相当する。

【0237】つぎに、算出された符号  $\alpha \#$  が、通信回路 841 および送信回路 855 を通じて、通信相手へ送信される (S803)。つづいて、通信相手が送信した符号  $\beta \# = g \beta \bmod (p)$  が、受信回路 854 によって受信され、通信回路 841 を通じて、鍵演算部 857 へ送られる (S804)。つぎに、鍵演算部 857 は、鍵  $K = g \alpha \beta \bmod (p)$  を算出する (S805)。その後、鍵演算部 857 は、算出した鍵 K を、通信相手の識別番号 (例えば、電話番号) とともに、メモリ 858 へ記録する (S806)。

【0238】つぎに、鍵演算部 857 は、鍵 K を暗号化回路 851 および復号化回路 852 へ供給することによ

り、鍵 K を共通鍵とする暗号通信を実現する (S808)。ステップ S808 の処理は、通信が終了するまで継続される (S809)。ステップ S801 において、通信相手が新規でないと判定されれば、鍵演算部 857 は、鍵 K を算出することなく、メモリ 858 へ記録されている鍵 K を読み出し (S807)、ステップ S808、S809 の処理を実行する。ステップ S801 の判定は、メモリ 858 に記録が存在するか否かにもとづいて行うことができる。

【0239】以上のように、通信相手と識別符号を交換することにより生成された共通鍵にもとづいて暗号通信が行われるので、通信内容の漏洩を防止しつつ、任意の通信相手との通信を実現することができる。なお、図 51 に手順において、ステップ S801 および S807 を除去して、通信が行われるごとに、鍵 K を算出することも可能である。

【0240】[10.4. 端末装置の別の例] 図 52 は、実施の形態 10 の端末装置の別の構成例を示すブロック図である。この端末装置 860 では、通信回路 861 が受信した受信信号は、低雑音増幅器 (Low Noise Amplifier) 862 で増幅され、VCO (Voltage Controlled Oscillator; 電圧制御型発振器) 864 に結合したミキサ 863 によって復調された後、ベースバンド回路 878 で処理される。また、ベースバンド回路 878 で処理された送信信号は、VCO 866 に結合したミキサ 865 で変調され、電力増幅器 (Power Amplifier) 867 で増幅された後、通信事業者設備へ送信される。

【0241】一方、無線 LAN 回路 871 が受信した受信信号は、低雑音増幅器 872 で増幅され、VCO 874 に結合したミキサ 873 によって復調された後、切替回路 870 を経由し、VCO 869 に結合したミキサ 868 によって変調される。変調された受信信号は、通信回路 861 のミキサ 863 を経て、ベースバンド回路 878 へ入力される。ベースバンド回路 878 へ入力された無線 LAN の受信信号は、復号化回路 852 によって復号化される。無線 LAN の送信信号は、ベースバンド回路 878 から暗号化回路 851 および切替回路 856 を経て、ベースバンド回路 879 へ入力される。その後、この送信信号は、VCO 766 に結合したミキサ 875 で変調され、電力増幅器 877 で増幅された後に送信される。

【0242】以上のように、図 52 の端末装置 860 は、無線 LAN 回路へ入力された受信信号が復調された後に、変調されて通信回路 861 へ入力される。図 53 が示すように、ミキサ 858 は、復調された無線 LAN の受信信号を、通信回路用帯域内に設定された特定範囲 (図 53 に「特別バンド」と記される) 内の周波数  $f$  を有する搬送波を用いて変調する。このため、無線 LAN の受信信号の周波数  $f$  が、無線 LAN 回路用帯域内のいずれの範囲にあっても、通信回路 861 には、周波数  $f$

が特別バンドの範囲内にある変調波が入力される。

【0243】仮に、無線LANの受信信号を復調することなく、周波数の変換のみを行って通信回路861へ入力した場合には、図54が示すように、通信回路用バンドを広く確保する必要がある。これに対して、図52の端末装置860では、通信回路用バンドを広く確保する必要がなく、通信回路861の周波数帯域の使用効率を高めることができるという利点が得られる。

【0244】図49または図52に例示されるように、通信回路と無線LAN回路とが選択自在に結合した端末装置では、図55が示すように、通信事業者設備を媒介とした通信経路と無線LANとを結合することも可能となる。すなわち、無線LANを形成している複数の端末装置850a～850cの一部である端末装置850cの遠距離通信部847の通信回路を通じて、別の端末装置850aが通信事業者設備を媒介とした通信を行うことができる。このように、電波が侵入し難い地下街などにある端末装置が、通信事業者設備を媒介した通信を行うことも可能である。通信事業者設備を媒介とした通信経路と無線LANとを結合する端末装置（図55の例では、端末装置850c）の負担を軽くするために、この

ような通信は、緊急非常通信に限って許可してもよい。

【0245】また、無線LANを通じての通信を、すべて緊急非常通信に制限することも可能である。それによって、無線LANを媒介とした通信を中継する端末装置（図47の例では、端末装置840b、840c）の負担を軽減することができる。また、緊急非常通信では、通信内容の漏洩に対するセキュリティの重要性が低いので、暗号化のための回路を除去することも可能となる。なお、緊急非常通信とは、例えば生命、財産を脅かす緊急事態の発生にともなう救助の要請などを目的とした通信である。

【0246】[11. 実施の形態11] 地下街、ビルディングの中など、通常時には多数の群衆が集中することが想定される領域においても、例えば夜間など時間帯によっては群衆の密度は低減する。実施の形態11では、電波が侵入し難い領域で、群衆の密度が低い場合にも、無線LANを媒介とした通信を可能にする通信方法について説明する。

【0247】図56は、実施の形態による通信方法を示す説明図である。この通信方法では、地下街などの電波が侵入し難い領域に、無線LANの形成を可能にする端末装置1050a、1050bが設置される。端末装置1050a、1050bは、好ましくは公衆電話機であり、例えば地下街の商店の入り口付近に設置される。この場合には、端末装置1050a、1050bは、近距離通信部848とともに、公衆電話機の本来の機能を達成する遠距離通信部1057を備える。群衆の密度が低い場合でも、端末装置850aと端末装置850bとが、端末装置1050a、1050bの近距離通信部8

48を中継することにより、無線LANを媒介した通信を行うことができる。

【0248】[12. 実施の形態12] 実施の形態12では、以上の実施の形態で説明した半導体素子401、符号化回路402および比較回路403に関し、さらに望ましい形態について説明する。

【0249】[12.1. 半導体素子の例] 図57は、半導体素子401の好ましい一例を示す回路図である。この半導体素子401aは、基板の上にマトリクス状に配列された複数の（図57の例では、 $4 \times 4$ 個＝16個の）TFT101を備えている。基板の上には、さらに、複数のワード線WL1～WL4、および、複数のビット線BL1～BL4が、それぞれ、横方向および縦方向に配列されている。

【0250】ワード線WL1～WL4の各々には、図上横一列に配列する4個のTFT101のゲート電極が共通に接続されている。一方、ビット線BL1～BL4の各々には、図上縦一列に配列する4個のTFT101のドレイン電極が共通に接続されている。16個のTFT101のソース電極は、正電源線へ共通に接続されている。また、ビット線BL1～BL4の各々の一端はビット線負荷7を通じて接地電源線へ接続されている。

【0251】ビット線負荷7の接地線とは反対側の一端には、アナログ信号Anを取り出すための配線18が接続されている。さらに、ビット線BL1～BL4の各々の他端には、パッド15が接続されており、ワード線WL1～WL4の各々の一端には、パッド16が接続されている。

【0252】半導体素子401aは、以上のように構成されるので、ワード線WL1～WL4の中の一つに、所定の高さのゲート電圧を付与することにより、そのワード線に接続された4個のTFT101に、ドレイン電流Id1～Id4が、それぞれ流れる。ドレイン電流Id1～Id4は、それぞれ、ビット線負荷17を流れるので、ビット線BL1～BL4に接続された配線18には、ドレイン電流Id1～Id4に比例した電位が発生する。この4個の電位がアナログ信号Anとして外部へ出力される。ワード線WL1～WL4に、順次、ゲート電圧を付与することにより、合計16個の電位を、アナログ信号Anとして取り出すことができる。

【0253】16個のアナログ信号Anは、符号化回路402によって符号化されることにより、例えば、図58が例示するように、16ビットのデジタル信号へ変換される。図58は、符号のもとになるTFT101と、それに接続されるビット線BL1～BL4およびワード線WL1～WL4との関係がわかるように、16ビットの符号をマトリクス状に配列して示している。

【0254】[12.2. 符号化回路および比較回路の例] 図59は、図1に示した半導体基板CH3（またはCH1）を半導体基板とする半導体装置の好ましい形態を示

すブロック図である。この半導体装置404aは、図57に示した半導体素子401aを備えている。半導体装置404aには、半導体素子401aに備わる複数のワード線WL1~WL4の任意の一つを、アドレス信号Adrにもとづいて駆動するデコーダ・ドライバ410が備わっている。アドレス信号Adrは、入力端子を通じて外部から入力することが可能である。

【0255】また、符号化回路402が出力する符号Cdは、比較回路403へ入力されるだけでなく、バッファ回路411を介して、外部へも出力される。それにより、限られた範囲の者が、識別符号Cdをあらかじめ知ることが可能となる。バッファ回路411が備わるので、符号化回路402が出力する識別符号Cdとは異なる符号を、識別符号Cdの出力端子を通じて外部から比較回路403へ入力するという不正行為を防止することができる。

【0256】半導体素子401aには、パッド15、16が備わるので、半導体装置404aを製造する過程の中では、これらのパッド15、16に探針を当てることにより、アナログ信号Anを直接に読み出すことも可能である。読み出されたアナログ信号Anは、符号化回路402と同一の特性を持った装置を用いて、識別符号Cdへと変換することができ、それにより、識別符号Cdを得ることも可能である。したがって、識別符号Cdの読み出しが、半導体装置404aの製造工場以外で行われる必要がなければ、アドレス信号Adrの入力端子、識別符号Cdの出力端子、および、バッファ回路411は、除去してもよい。

【0257】比較回路403は、入力端子を通じて入力される記憶符号Coを、識別符号Cdと比較する際に、デコーダ・ドライバ410へ、アドレス信号Adrを入力する。それにより、半導体装置404aが駆動され、アナログ信号Anが読み出されるので、外部からアドレス信号Adrを入力しなくても、識別符号Cdと記憶符号Coとの間の比較を行うことが可能となる。

【0258】図60は、符号化回路402の好ましい形態を示す回路図であり、代表としてビット線BL1に接続される部分を描いている。他のビット線BL2~BL4にも、図60と同様の回路部分が接続されている。この符号化回路402aには、センスアンプ190が備わっている。センスアンプ190は、配線18の電位と、トランジスタ192、193が生成する基準電位Vrefとを比較して、ハイレベルまたはロウレベルの信号を生成し、識別符号Cdの1ビット分（例えば、ビット線BL1に対応した識別符号Cd(1)）として出力する。

【0259】センスアンプ190では、NMOSトランジスタ194とPMOSトランジスタ195の直列回路、および、NMOSトランジスタ196とPMOSトランジスタ197の直列回路が、接地電源線と正電源線との間に介挿されている。そして、PMOSトランジスタ195のゲート電極

とドレイン電極、および、PMOSトランジスタ197のゲート電極が、互いに接続されることにより、カレントミラー回路が形成されている。

【0260】TFT101を流れるドレイン電流は、約1pA ( $10^{-12}$ A) ~ 約1 $\mu$ Aの範囲内の低い値である。したがって、ビット線負荷17として、NMOSトランジスタを用い、そのゲート電極に一定電位を印加することによって、そのドレイン電流を、約1nA ( $10^{-9}$ A)程度に設定するのが望ましい。それによって、センスアンプ190の感度が高められる。ドレイン電流を約1nA程度に設定する上で、ゲート電位は、接地電位とするのが望ましい。

【0261】NMOSトランジスタ192とPMOSトランジスタ193の直列回路が、接地電源線と正電源線との間に介挿されており、これらの二つのトランジスタの接続部から基準電位Vrefが取り出される。NMOSトランジスタ192およびPMOSトランジスタ193のゲート電極には、それぞれ接地電源線の電位および正電源線の電位などの一定電位が供給される。配線18の電位と基準電位Vrefとが比較されることは、TFT101のドレイン電流とNMOSトランジスタ192とPMOSトランジスタ193の直列回路を流れる基準電流Ir（またはその定数倍）とが比較されることと等価である。

【0262】安定した比較を行う上では、図60に描かれるTFT101以外のトランジスタは、TFT型ではないバルク型のトランジスタとして構成されるのが望ましい。TFT101以外のトランジスタを、TFT101と同じく多結晶TFTとして形成するのであれば、それらのドレイン電流の大きさを安定なものとするために、それらのゲート長およびゲート幅は、TFT101のゲート長およびゲート幅よりも大きく設定されるのが望ましい。

【0263】[12.3. 半導体素子の別の例] 半導体素子401は、多結晶型のTFT101を備える代わりに、例えば、多結晶体の抵抗素子、あるいは、多結晶体のキャパシタ（容量素子）を備えてもよい。以下では、そのような例について説明する。

【0264】図61は、半導体素子401が多結晶体の抵抗素子を備える例を示す回路図である。この半導体素子401bでは、基板の上にマトリクス状に配列された複数の（図61の例では、 $4 \times 4$ 個=16個の）抵抗素子43を備えている。抵抗素子43では、その抵抗体が、多結晶半導体、例えば多結晶シリコンで形成されている。このため、抵抗素子43では、抵抗値がランダムにばらつく。

【0265】基板の上には、さらに、複数のワード線WL1~WL4、および、複数のビット線BL1~BL4が、それぞれ横方向および縦方向に配列されている。

【0266】ワード線WL1~WL4の各々には、図上横一列に配列する4個の抵抗素子43の一端が共通に接続されている。一方、ビット線BL1~BL4の各々に

は、図上縦一列に配列する4個の抵抗素子43の他端が共通に接続されている。また、ビット線BL1～BL4の各々の一端はビット線負荷としてのNMOSトランジスタ48を通じて接地電源線へ接続されている。NMOSトランジスタ48のゲート電極は、例えば、接地電源線に接続される。

【0267】NMOSトランジスタ48のドレイン電極には、アナログ信号Anを取り出すための配線49が接続されている。さらに、ビット線BL1～BL4の各々の他端には、パッド15が接続されており、ワード線WL1～WL4の各々の一端には、パッド16が接続されている。

【0268】半導体素子401bは、以上のように構成されるので、ワード線WL1～WL4の中の一つに、所定の高さのゲート電圧を付与することにより、そのワード線に接続された4個の抵抗素子43に電流が流れる。これらの電流は、NMOSトランジスタ48を流れるので、ビット線BL1～BL4に接続された配線49の各々には、抵抗素子43を流れる電流に比例した電位が発生する。この4個の電位がアナログ信号Anとして外部へ出力される。ワード線WL1～WL4に、順次、所定の電位を付与することにより、合計16個の電位を、アナログ信号Anとして取り出すことができる。アナログ信号Anは、抵抗素子43の抵抗のばらつきに対応したランダムな値として得られる。

【0269】パッド15、16が備わるので、探針を用いて半導体素子401bの製造工程の中で、アナログ信号Anを読み出すことも可能である。また、抵抗素子43は、一次元マトリクス状に配列され、すべての抵抗素子43の一端が単一のワード線に接続されてもよい。アナログ信号Anのばらつきを大きくするためには、抵抗素子43が有する多結晶体の長さおよび幅を、ゲート長Lおよびゲート幅Wに対する最適条件と同様の範囲に設定するとよい。

【0270】[12.4. 半導体素子のさらに別の例] 図62は、半導体素子401が多結晶体の容量素子を備える例を示す回路図である。この半導体素子401cでは、基板の上にマトリクス状に配列された複数の(図61の例では、 $4 \times 4$ 個=16個の)容量素子91とMOSトランジスタ90の直列回路を備えている。容量素子91には、多結晶誘電体、例えばBST(BaxSr<sub>1-x</sub>TiO<sub>3</sub>)などのペロブスカイト型の多結晶誘電体が備わっている。このため、容量素子91では、容量値がランダムにばらつく。

【0271】基板の上には、さらに、複数のワード線WL1～WL4、および、複数のビット線BL1～BL4が、それぞれ横方向および縦方向に配列されている。ワード線WL1～WL4の各々には、図上横一列に配列する4個の直列回路に属するMOSトランジスタ90のゲート電極が共通に接続されている。一方、ビット線BL1

～BL4の各々には、図上縦一列に配列する4個の直列回路に属するMOSトランジスタ90のソース電極およびドレイン電極の一方電極が、共通に接続されている。16個の直列回路に属する容量素子91の一端は、接地電源線に接続されている。ビット線BL1～BL4の各々の他端には、パッド15が接続されており、ワード線WL1～WL4の各々の一端には、パッド16が接続されている。

【0272】半導体素子401cは、以上のように構成されるので、ワード線WL1～WL4の中の一つに、所定の高さのゲート電圧を付与することにより、そのワード線に接続された4個のMOSトランジスタをオンさせることができる。オンしたMOSトランジスタを通じて、4個の容量素子91の他端が、ビット線BL1～BL4に電気的に接続される。このときビット線BL1～BL4を通じて、4個の容量素子91の容量(キャパシタンス)を計測することができる。例えば、一定時間にわたって電流を供給したときの電位を計測することができ、この電位をアナログ信号Anとして取り出すとよい。この電位には、容量素子91の容量が反映されている。

【0273】ワード線WL1～WL4に、順次、所定のゲート電圧を付与することにより、合計16個の電位を、アナログ信号Anとして取り出すことができる。アナログ信号Anは、容量素子91の容量のばらつきに対応したランダムな値として得られる。パッド15、16が備わるので、探針を用いて半導体素子401cの製造工程の中で、アナログ信号Anを読み出すことも可能である。また、容量素子91とMOSトランジスタ90との直列回路は、一次元マトリクス状に配列され、すべてのMOSトランジスタ90のゲート電極が単一のワード線に接続されてもよい。

【0274】アナログ信号Anのばらつきを大きくするためには、容量素子91が有する多結晶誘電体の長さおよび幅を、ゲート長Lおよびゲート幅Wに対する最適条件と同様の範囲に設定するとよい。BSTでは、その膜厚が100nmであるとき、シリコン酸化膜に換算した膜厚は、約0.5nmである。したがって、電極に面するBSTの形状が、一辺が0.3 $\mu$ mの正方形であるとする、その容量は6.2fF程度となる。結晶粒径(平均値)が膜厚に相当する100nmに設定された最適な場合は、その容量は-30%～+30%の範囲、すなわち、4.3fF～8.1fFの範囲にばらつく。この値は、識別として利用するのに十分な大きさのばらつきであると云える。

【0275】[12.5. 比較回路のさらに別の例] 図63は、図1に示した半導体基板CH3(またはCH1)を半導体基板とする半導体装置の好ましい別の形態を示すブロック図である。この半導体装置404dが備える比較回路403aは、識別符号Cdと記憶符号Coとの完全一致性だけでなく、あらかじめ定められた範囲での近似性をも判定することができるように構成されている。

判定の基準値SLは、入力端子を通じて半導体装置404dの外部から入力することができる。

【0276】このことを可能にするために、比較回路403aは、ワード線WLの電位をスweepするスweep回路200を備えている。ワード線WLの電位がスweepされることによって変化する識別符号Cdは、近似度算出回路199によって、入力符号メモリ198に保持される記憶符号Coの対応する一部と比較される。近似度算出回路199は、比較を通じて算出した双方の符号の間の近似度VAを、評価回路210へ伝達する。評価回路210は、近似度VAを基準値SLと比較することによって、近似度VAが一定以上であるか否かを判定し、その結果を判定信号VBとして出力する。

【0277】判定信号VBは、デコーダ・ドライバ410が駆動する一つのワード線WLごとに個別に得られる。アドレス発生回路441は、すべてのワード線WLを、一つずつ順に指定するアドレス信号をデコーダ・ドライバ410へ伝達する。それにより、すべてのワード線WLに対応した複数の判定信号VBが、一つずつ順に得られる。

【0278】総合判定回路220は、すべてのワード線WLに対応した複数の判定信号VBにもとづいて、すべてのワード線WLに対応した全ビットの符号Cdと、全ビットの符号Coとの間の近似性を判定し、その結果を表現する判定信号Enを出力する。基準値SLを適切に設定することにより、近似性の判定として、もっとも厳しい完全一致性の判定を選択することも可能である。ワード線が単一であれば、総合判定回路220は不要であり、判定信号VBがそのまま判定信号Enとして出力される。

【0279】制御回路442は、入力端子を通じて入力される指示信号Stにตอบสนองして、比較回路403aの各要素の動作を開始させるとともに、各要素の動作を所定の手順に沿うように制御する。特に、制御回路442からスweep回路200へと、スweepを行うか否かを指示する制御信号であるスweepスイッチ信号SSが伝達される。なお、近似度算出回路199、評価回路210、および、総合判定回路220は、判定回路440を構成する。

【0280】

【発明の効果】第1の発明の装置では、半導体基板を識別するための符号が、別の半導体基板に記憶されているので、本装置が組み込まれた応用機器を、半導体基板を取り替えて使用するという不正行為を、これらの符号を照合することによって防止することができる。

【0281】第2の発明の装置では、メモリがOTPROMに符号を記憶するので、メモリに記憶される符号の不正な変更に対する障壁が高い。

【0282】第3の発明の装置では、半導体素子の電気的特性のばらつきを利用して識別符号が生成されるので、量産される多数の本装置の間で、同一工程で製造さ

れた半導体素子を用いることができる。このため、装置の製造が簡略化される。また、識別符号のもとになる半導体素子の電気的特性を外部から変更することができないので、識別符号の不正な変更に対する障壁が高い。

【0283】第4の発明の装置では、半導体素子が多結晶体を有し、その結晶構造のばらつきを利用して識別符号が生成されるので、同一工程で製造された半導体素子の間での電気的特性のばらつきが大きい。このため、量産される多数の本装置の間で、互いに識別符号が一致しないようにすることが容易である。

【0284】第5の発明の装置では、符号生成部がOTPROMに識別符号を記憶するので、符号生成部が生成する識別符号の不正な変更に対する障壁が高い。

【0285】第6の発明の装置では、比較回路によって、符号の一致性の判定が行われるので、判定信号を認証に利用することができる。

【0286】第7の発明の装置では、符号生成部が形成されている半導体基板に比較回路が形成されているので、同一の半導体基板の中で符号生成部から比較回路へ入力される識別符号を外部から不正に変更することができない。このため、不正使用に対する障壁が、さらに高められる。

【0287】第8の発明の装置では、異なる半導体基板の間で、暗号化された形式で符号がやりとりされるので、外部から符号を読み取ることができない。このため、不正使用に対する障壁がさらに高められる。

【0288】第9の発明の装置では、半導体素子の電気的特性のばらつきを利用して鍵が生成されるので、量産される多数の本装置の間で、同一工程で製造された半導体素子を用いることができる。このため、装置の製造が簡略化される。また、鍵のもとになる半導体素子の電気的特性を外部から変更することができないので、鍵の不正な変更に対する障壁が高い。

【0289】第10の発明の装置では、半導体素子が多結晶体を有し、その結晶構造のばらつきを利用して鍵が生成されるので、同一工程で製造された半導体素子の間での電気的特性のばらつきが大きい。このため、量産される多数の本装置の間で、互いに鍵が一致しないようにすることが容易である。

【0290】第11の発明の装置では、鍵生成部が、OTPROMに鍵を記憶するので、鍵生成部が生成する鍵の不正な変更に対する障壁が高い。

【0291】第12の発明の装置では、スイッチ回路が備わるので、半導体基板から出力される識別符号を記憶符号に見せかけて、そのまま同一の半導体基板へ入力することによってなされる不正使用を防止することができる。

【0292】第13の発明の装置では、比較回路の判定にもとづいて動作または非動作となる回路部分を含む所定回路が備わるので、所定回路を応用機器の機能を実現



する回路の一部とすることにより、比較の結果に応じて、応用機器の所定の動作を許可および不許可することができる。

【0293】第14の発明の装置では、符号生成部および比較回路が形成されている半導体基板の一つに所定回路が形成されているので、同一の半導体基板の中で比較回路から所定回路へ入力される判定信号については、これを外部から入力することができない。このため、不正使用に対する障壁が、さらに高められる。

【0294】第15の発明の装置では、二つの半導体基板の一方に符号生成部が形成され、他方にメモリが形成され、一方の半導体基板に固有の識別符号に一致する符号が他方の半導体基板に記憶されるという、もっとも簡素な構成を有する。このため、装置の製造が容易であり、かつ装置を小型化することが可能である。

【0295】第16の発明の装置では、二つの半導体基板のいずれにも符号生成部とメモリとが形成され、二つの半導体基板が、互いに相手側の識別符号に一致する符号を記憶するので、半導体基板の個数を最小に抑えつつ、不正使用に対する障壁をさらに高めることができる。

【0296】第17の発明の装置では、暗号化した形式でデータを外部との間でやりとりすることができるので、データが表現する情報の漏洩に対する障壁が高い。しかも、半導体素子の電気的特性のばらつきを利用して暗号化のための鍵が生成されるので、量産される多数の本装置の間で、同一工程で製造された半導体素子を用いることができる。このため、装置の製造が簡略化される。また、鍵のもとになる半導体素子の電気的特性を外部から変更することができないので、鍵の不正な変更に対する障壁が高い。

【0297】第18の発明の装置では、本体部に着脱自在の補助部に鍵生成部が組み込まれているので、複数の本体部に対して同一の鍵を使用することが可能である。

【0298】第19の発明の装置では、鍵生成部がICカードに組み込まれているので、携帯に便利である。

【0299】第20の発明の装置では、半導体素子が多結晶性を有し、その結晶構造のばらつきを利用して鍵が生成されるので、同一工程で製造された半導体素子の間での電気的特性のばらつきが大きい。このため、量産される多数の本装置の間で、互いに鍵が一致しないようにすることが容易である。

【0300】第21の発明の装置では、比較回路の判定が不一致を示すときに送信または受信の少なくとも一方を停止する通信回路が備わるので、半導体基板を取り替えて通信に使用するという不正行為が、通信事業者設備等による処理を待つことなく端末装置自体の働きによって自動的に抑えられる。

【0301】第22の発明の装置では、各判定信号が送信されるので、通信事業者設備等が判定信号にもとづい

て認証処理を行うことにより、半導体基板を取り替えて通信に使用するという不正行為を防止することができる。

【0302】第23の発明の装置では、各識別符号と各記憶符号とが送信されるので、通信事業者設備等がこれらの符号を比較し、その結果にもとづいて認証処理を行うことにより、半導体基板を取り替えて通信に使用するという不正行為を防止することができる。

【0303】第24の発明の装置では、本体部に着脱自在の補助部にメモリが組み込まれているので、本体部と補助部とが結合したとき、および結合していないときの二通りの間で異なるレベルでの認証を通信事業者設備等が行うことができる。例えば、通信事業者設備は、本体部と補助部とが結合したときの高レベルの認証によって、それ以前の通信に対する通信料金を、裏付けられたものとして記録することができ、それにより端末装置の紛失を装って料金支払いの義務を逃れる違法行為を防止することが可能となる。

【0304】第25の発明の装置では、暗号化された形式で、識別符号および記憶符号が送信されるので、これらの符号の漏洩に対する障壁が高い。

【0305】第26の発明の装置では、第1鍵生成部と第1暗号化回路とが、符号化回路とともに単一の半導体基板に形成されているので、識別符号および第1鍵の漏洩に対する障壁がさらに高められる。

【0306】第27の発明の装置では、第2鍵生成部と第2暗号化回路とが、メモリとともに単一の半導体基板に形成されているので、記憶符号および第2鍵の漏洩に対する障壁がさらに高められる。

【0307】第28の発明の装置では、補助部が本体部の電池を充電する充電器であるので、使用者に特別の手間を要求することなく、本体部と補助部との結合が定期的に行われる。

【0308】第29の発明の装置では、補助部がICカードであり、携帯に便利である。また、本体部と補助部の間で、無線で符号がやり取りされるので、ICカードを本体部とともに携帯するだけで、双方の結合が実現する。

【0309】第30の発明の装置では、符号生成部が形成されている半導体基板の一つに通信回路が形成されているので、同一の半導体基板の中で通信回路へ入力される判定信号または符号については、これを外部から入力することができない。このため、不正使用に対する障壁が、さらに高められる。

【0310】第31の発明の装置では、本装置を携帯する群衆が集合ないし通行する空間において、群衆の中の少なくとも一部の複数人が携帯する本装置の間で無線通信網を形成することができ、それにより、通信事業者設備を媒介した無線通信を行い得ない領域、例えば地下街などが上記空間の中にあっても、上記空間の中での通信



が可能となる。

【0311】第32の発明の装置では、切替回路が備わるので、無線通信網を通じての他者どうしの通信が中継されるだけでなく、本装置の使用者自身が無線通信網による通信を行うことができる。

【0312】第33の発明の装置では、通信相手と符号を交換することにより共通鍵が設定され、当該共通鍵にもとづいて暗号化された形式で通信信号がやりとりされるので、任意の通信相手との通信内容の漏洩に対する障壁が高い。

【0313】第34の発明の装置では、半導体素子の電気的特性のばらつきを利用して、共通鍵のもとになる符号が生成されるので、量産される多数の本装置の間で、同一工程で製造された半導体素子を用いることができる。このため、装置の製造が簡略化される。また、符号のもとになる半導体素子の電気的特性を外から変更することができないので、符号の不正な変更に対する障壁が高い。

【0314】第35の発明の装置では、半導体素子が多結晶を有し、その結晶構造のばらつきを利用して符号が生成されるので、同一工程で製造された半導体素子の間での電気的特性のばらつきが大きい。このため、量産される多数の本装置の間で、互いに符号が一致しないようにすることが容易である。

【0315】第36の発明の装置では、符号生成部がOTPROMに符号を記憶するので、符号生成部が生成する符号の不正な変更に対する障壁が高い。

【0316】第37の発明の装置では、無線通信網回路が受信した信号が、復調された後に変調されて通信回路へ伝えられるので、通信回路の周波数帯域の使用効率が高められる。

【0317】第38の発明の方法では、端末装置が送信する各判定信号が認証に用いられるので、半導体基板を取り替えて通信に使用するという不正行為を防止することができる。

【0318】第39の発明の方法では、端末装置が送信する各識別符号および各記憶符号が認証に用いられるので、半導体基板を取り替えて通信に使用するという不正行為を防止することができる。

【0319】第40の発明の方法では、受信した各識別符号および各記憶符号が記録されるので、不正使用による犯罪を事前に抑止する効果が得られる。また、不正使用があった場合に、記録している各符号を不正使用者の特定に役立てることが可能となる。

【0320】第41の発明の方法では、認証工程で認証を行わない場合、すなわち使用者が不正使用者である可能性のある場合に、受信した各識別符号および各記憶符号が記録されるので、記録した各符号を不正使用者の特定に役立てることができる。

【0321】第42の発明の方法では、本体部と補助部

とが結合したとき、および結合していないときの二通りの間で異なるレベルでの認証が行われる。本体部と補助部とが結合したときになされる高位の認証は、識別符号と記憶符号のいずれもが、登録された符号と一致する場合に限ってなされるので、端末装置が正当に使用されている確度がより高いことを証明するものとなる。したがって、通信事業者設備は、手続の重要性に応じた認証を使い分けることが可能となる。

【0322】第43の発明の方法では、補助部が本体部に装着された状態で通信を行うことにより、登録すべき記憶符号が通信事業者設備へ送られるので、端末装置が使用者の手に渡るより前には、識別符号のみを登録すれば足りる。

【0323】第44の発明の方法では、第2登録符号を変更することが可能であるので、使用者は、端末装置を入手後に必要に応じて補助部を交換することができる。

【0324】第45の発明の方法では、本体部と補助部とが結合したとき、および結合していないときの二通りの間で異なるレベルでの認証が行われる。本体部と補助部とが結合したときになされる高位の認証は、識別符号と記憶符号のいずれもが、登録された符号と一致する場合に限ってなされるので、端末装置が正当に使用されている確度がより高いことを証明するものとなる。したがって、通信事業者設備は、手続の重要性に応じた認証を使い分けることが可能となる。しかも、暗号化された形式で、識別符号および記憶符号が送信されるので、これらの符号の漏洩に対する障壁が高い。

【0325】第46の発明の方法では、補助部が本体部に装着された状態で通信を行うことにより、登録すべき記憶符号が通信事業者設備へ送られるので、端末装置が使用者の手に渡るより前には、識別符号のみを登録すれば足りる。

【0326】第47の発明の方法では、第2登録符号を変更することが可能であるので、使用者は、端末装置を入手後に必要に応じて補助部を交換することができる。

【0327】第48の発明の方法では、高位の認証工程で認証を行わない場合、すなわち使用者が不正使用者である可能性が高い場合に、受信した各識別符号および各記憶符号が記録されるので、記録した各符号を不正使用者の特定に役立てることができる。

【0328】第49の発明の方法では、高位認証工程において、高位の認証を行う場合、すなわち、使用者が正当使用者である可能性が高い場合には、それ以前の通信に対する通信料金を、裏付けられたものとして記録するので、端末装置の紛失を装って料金支払いの義務を逃れる違法行為を防止することが可能である。

【0329】第50の発明の方法では、補助部が本体部に装着されない状態でなされる通常の認証に、過去の高位の認証工程でなされた判断結果が反映されるので、商取引などの重要な手続を、通常の認証の下で行うことが

できる。

【0330】第51の発明の方法では、高位認証工程において、それ以前の通信によって行われた商取引の成立または不成立が、高位の認証を行うか否かに応じて記録されるので、端末装置の不正使用にもとづく不正な商取引による損害を解消ないし低減することができる。

【0331】第52の発明の方法では、認証工程において、認証を行うか否かに応じて通信が継続または中止されるので、端末装置の不正使用にもとづく通信を防止することができる。

【0332】第53の発明の方法では、所定の機能を有する端末装置を携帯する群衆が集合ないし通行する空間において、群衆の中の少なくとも一部の複数人が携帯する上記端末装置の間で無線通信網が形成され、それにより、通信事業者設備を媒介した無線通信を行い得ない領域、例えば地下街などが上記空間の中にあっても、上記空間の中での通信が実現する。

【0333】第54の発明の方法では、無線通信網を形成する複数の端末装置の一部が通信事業者設備を媒介した無線通信を行うことにより、上記複数の端末装置の他の一部が無線通信網と通信事業者設備とを媒介した通信を行うことが可能であるので、通信事業者設備を媒介した無線通信を行い得ない領域、例えば地下街などから、通信事業者設備を媒介した無線通信を行うことが可能となる。

【0334】第55の発明の方法では、通信相手と符号を交換することにより共通鍵が設定され、当該共通鍵にもとづいて暗号化された形式で通信信号がやりとりされるので、任意の通信相手との通信内容の漏洩に対する障壁が高い。

【0335】第56の発明の方法では、無線通信網を媒介した通信が、例えば生命、財産を脅かす緊急事態の発生にともなう救助の要請などの、緊急非常通信に限って可能とされるので、通信内容の漏洩を防止するための暗号化などの手順を要しない。

【0336】第57の発明の方法では、無線通信網の形成が可能な端末装置が、通信事業者設備を媒介した無線通信を行い得ない領域、例えば地下街などに設置されるので、上記領域において、所定の機能を有する端末装置を携帯する群衆の密度が低い場合でも、無線通信網を媒介した通信が可能となる。

#### 【図面の簡単な説明】

【図1】 実施の形態1の半導体装置のブロック図である。

【図2】 図1の符号生成部のブロック図である。

【図3】 図2の半導体素子の平面図である。

【図4】 図3の半導体素子のA-A切断線に沿った断面図である。

【図5】 図2の半導体素子の平面図である。

【図6】 図2の半導体素子の特性を表すグラフであ

る。

【図7】 図1の符号生成部の別の例のブロック図である。

【図8】 図1のメモリのブロック図である。

【図9】 実施の形態1の端末装置のブロック図である。

【図10】 図9の通信回路のブロック図である。

【図11】 図9の端末装置の使用に至るまでの手順の流れ図である。

10 【図12】 実施の形態1の通信システムのブロック図である。

【図13】 実施の形態2の半導体装置のブロック図である。

【図14】 実施の形態2の端末装置のブロック図である。

【図15】 図13の端末装置の使用に至るまでの手順の流れ図である。

【図16】 実施の形態3の端末装置のブロック図である。

20 【図17】 図16の端末装置を用いた通信方法の流れ図である。

【図18】 実施の形態3の端末装置の別の例のブロック図である。

【図19】 図18の端末装置を用いた通信方法の流れ図である。

【図20】 実施の形態4の端末装置のブロック図である。

【図21】 図20の端末装置を用いた通信方法の流れ図である。

30 【図22】 実施の形態4の端末装置の別の例のブロック図である。

【図23】 図22の端末装置を用いた通信方法の流れ図である。

【図24】 実施の形態5の半導体装置のブロック図である。

【図25】 図24の鍵生成部のブロック図である。

【図26】 図24の鍵生成部の別の例のブロック図である。

【図27】 図24の半導体装置を組み込んだ端末装置の使用に至るまでの手順の流れ図である。

40 【図28】 実施の形態5の半導体装置の別の例のブロック図である。

【図29】 図28の半導体装置を組み込んだ端末装置の使用に至るまでの手順の流れ図である。

【図30】 実施の形態6の半導体装置のブロック図である。

【図31】 実施の形態7の端末装置のブロック図である。

50 【図32】 実施の形態7の端末装置の別の例のブロック図である。

67

【図33】 実施の形態8の端末装置のブロック図である。

【図34】 図33の端末装置の使用に至るまでの手順の流れ図である。

【図35】 図34のステップS509の流れ図である。

【図36】 図34のステップS509の流れ図である。

【図37】 実施の形態9の端末装置のブロック図である。

【図38】 図37の端末装置の使用に至るまでの手順の流れ図である。

【図39】 図38のステップS709の流れ図である。

【図40】 図38のステップS709の流れ図である。

【図41】 図38のステップS709の別の例の流れ図である。

【図42】 図41のステップS742の流れ図である。

【図43】 図41のステップS742の流れ図である。

【図44】 図38のステップS709の別の例の流れ図である。

【図45】 図38のステップS709の別の例の流れ図である。

【図46】 実施の形態9の端末装置の別の例のブロック図である。

【図47】 実施の形態10の通信方法の説明図である。

【図48】 実施の形態10の端末装置のブロック図である。

【図49】 実施の形態10の端末装置の別の例のブロック図である。

【図50】 図49の鍵生成部のブロック図である。

【図51】 図49の端末装置による鍵生成の流れ図である。

【図52】 実施の形態10の端末装置のさらに別の例のブロック図である。

【図53】 図52の端末装置の動作説明図である。

68

【図54】 図53に対比される動作を示す説明図である。

【図55】 実施の形態10の通信方法の別の例の説明図である。

【図56】 実施の形態11の通信方法の説明図である。

【図57】 実施の形態12の半導体素子のブロック図である。

【図58】 図57の半導体素子の動作説明図である。

【図59】 実施の形態12の半導体装置のブロック図である。

【図60】 図59の符号化回路の一部のブロック図である。

【図61】 実施の形態12の半導体素子の別の例のブロック図である。

【図62】 実施の形態12の半導体素子のさらに別の例のブロック図である。

【図63】 実施の形態12の半導体素子の比較回路のブロック図である。

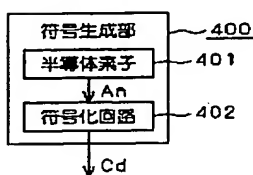
【図64】 従来の通信システムの処理を説明する図である。

【図65】 従来の通信端末のブロック図である。

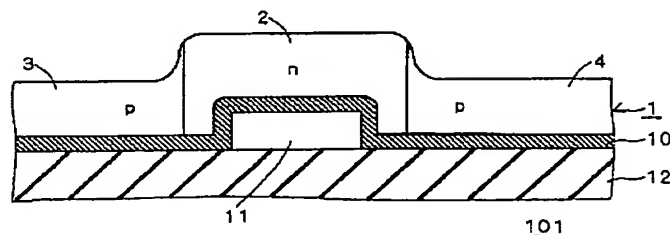
【符号の説明】

400 符号生成部、401 半導体素子、402 符号化回路、403 比較回路、405、405a 所定回路、601、654 メモリ、602 OTPROM、633、676、853 鍵生成部、631、851 暗号化回路、632、852 復号化回路、641 スイッチ回路、652、672、828、692 本体部、653、673、693 充電器（補助部）、655、675 通信事業者設備、694、695 通信インタフェース、829 ICカード（補助部）、841、861 通信回路、846、871 無線LAN回路（無線通信網回路）、856、870 切替回路、857 鍵演算部、868、873 ミキサ、Cd、Cd1、Cd2 識別符号、Co、Co1、Co2 記憶符号、CH1～CH6、CH10～CH13、CH20～CH23、CH40～CH42、CH50～CH52、CH70、CH71、CH90～CH92、CH100～CH104 半導体基板、K、K1、K2 鍵。

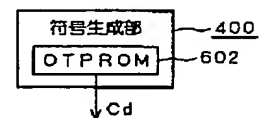
【図2】



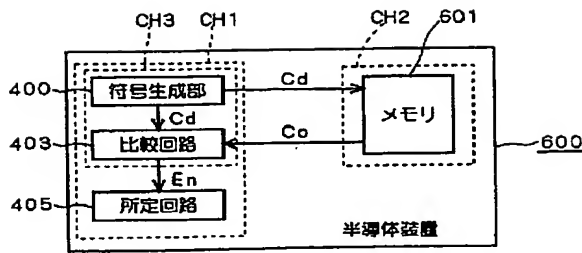
【図4】



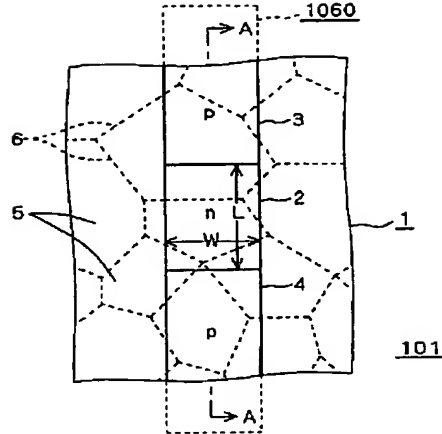
【図7】



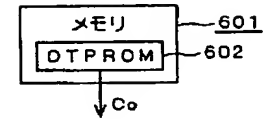
【図1】



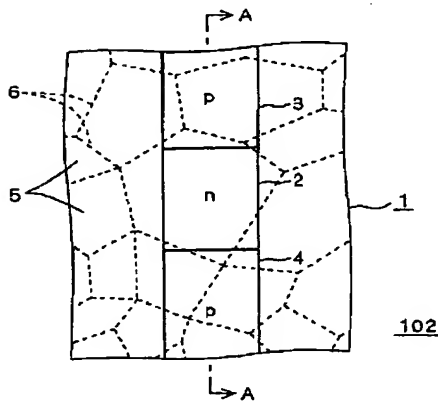
【図3】



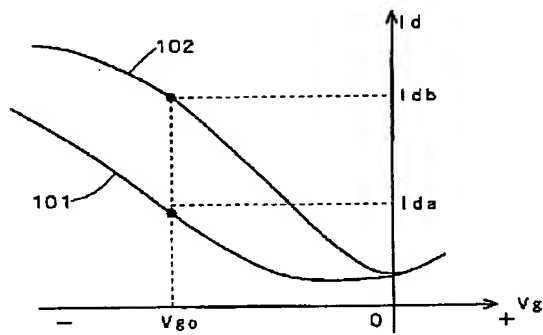
【図8】



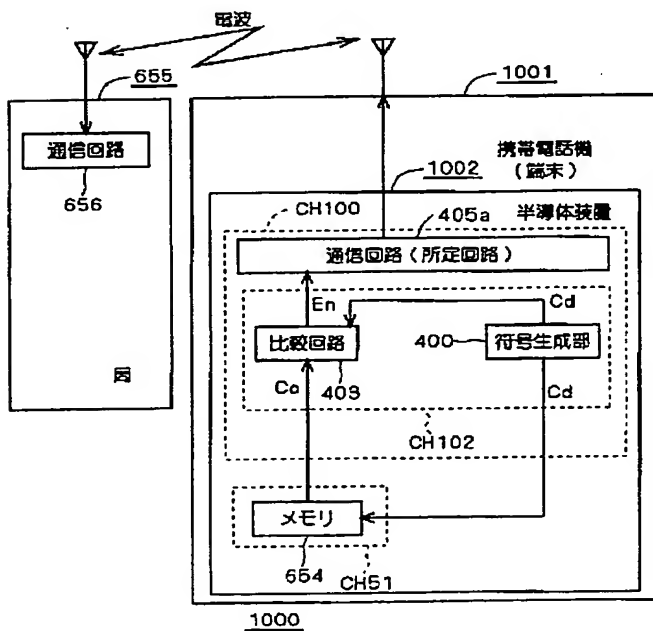
【図5】



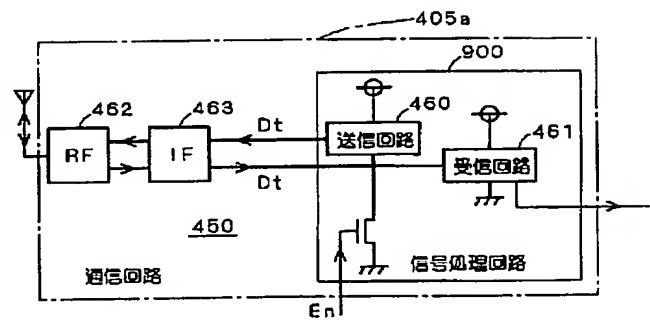
【図6】



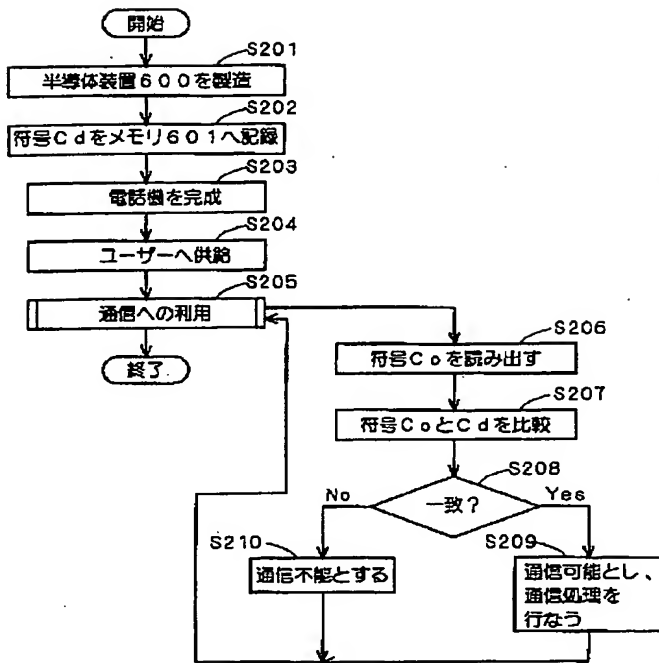
【図9】



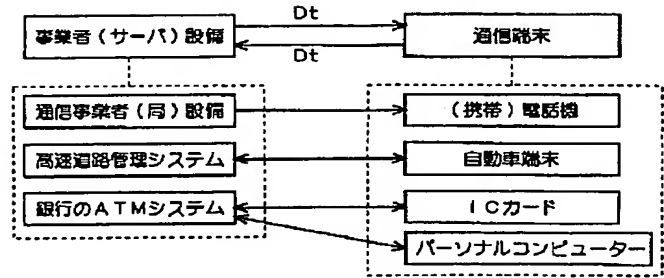
【図10】



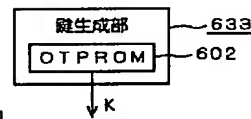
【図11】



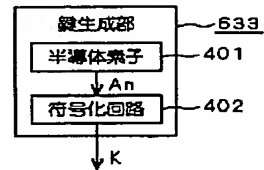
【図12】



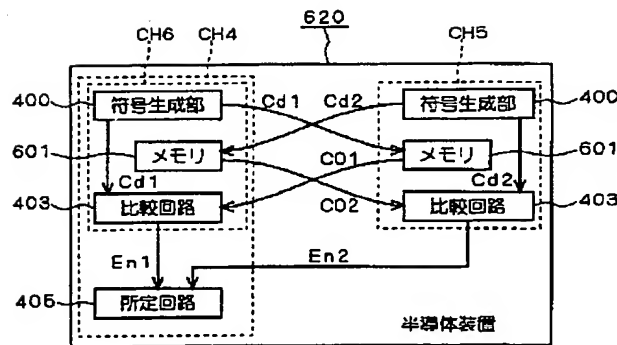
【図25】



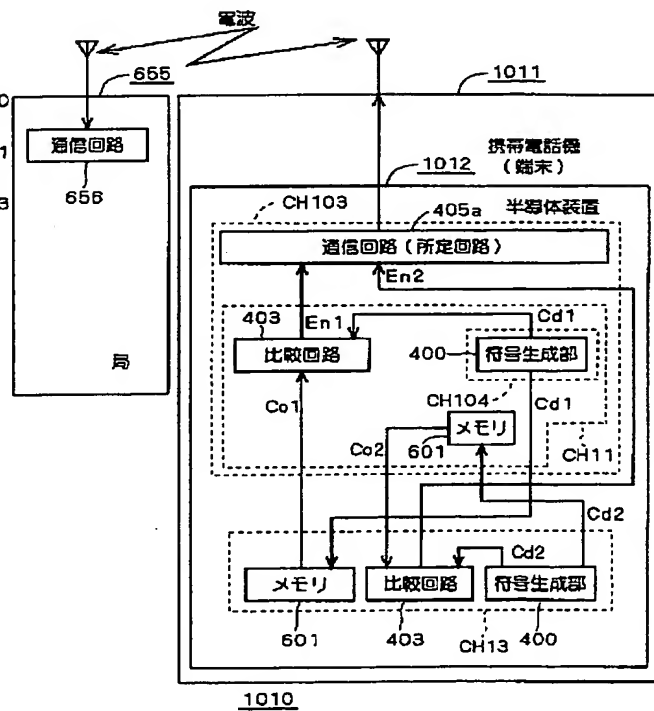
【図26】



【図13】

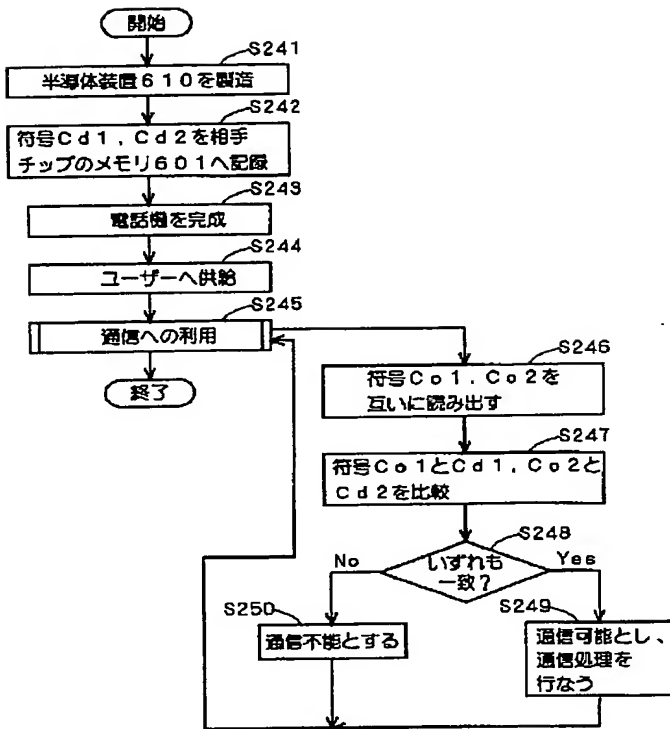


【図14】

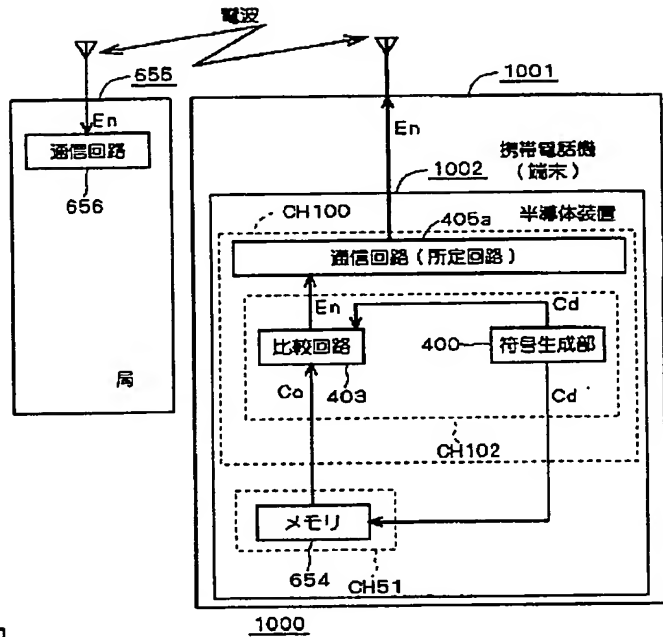




【図15】

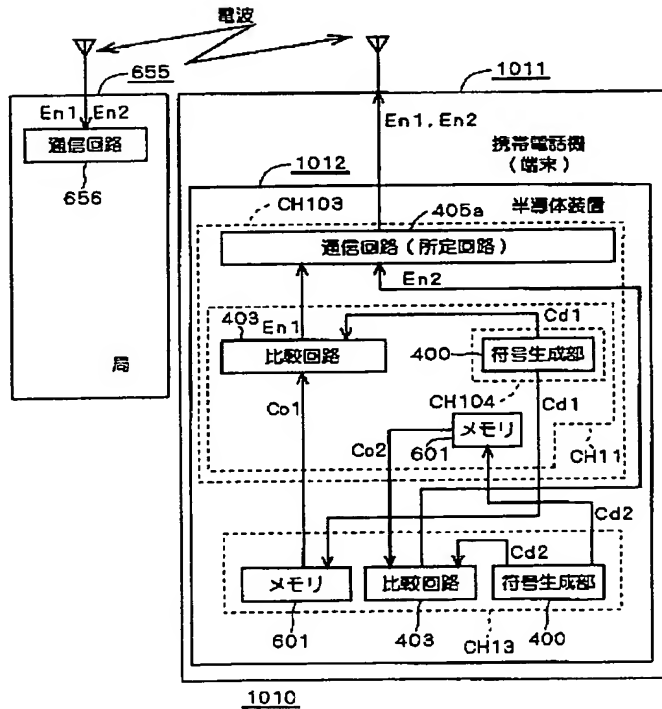
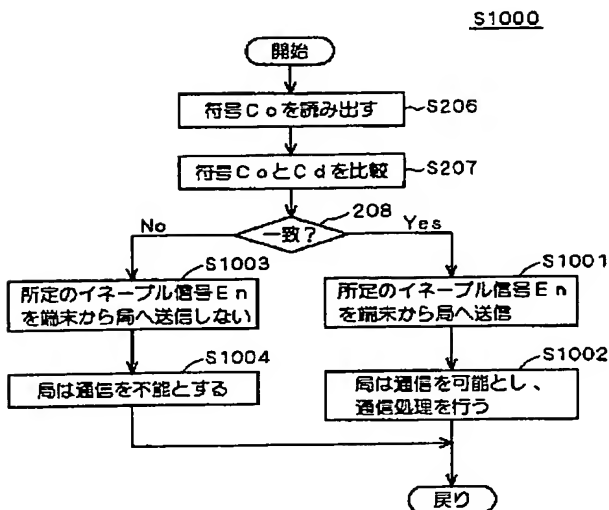


【図16】



【図17】

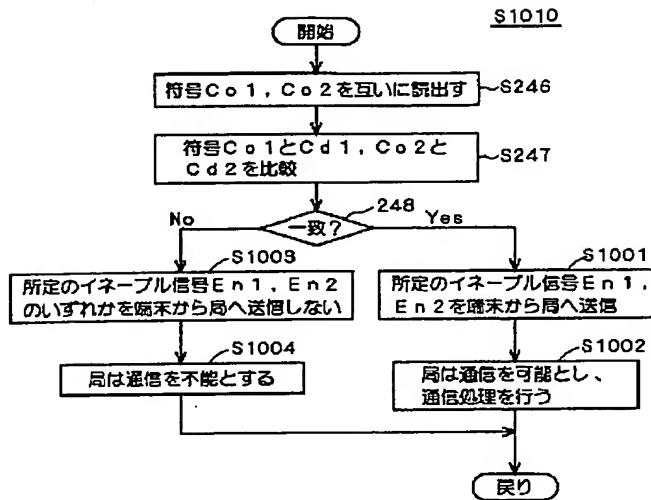
【図18】



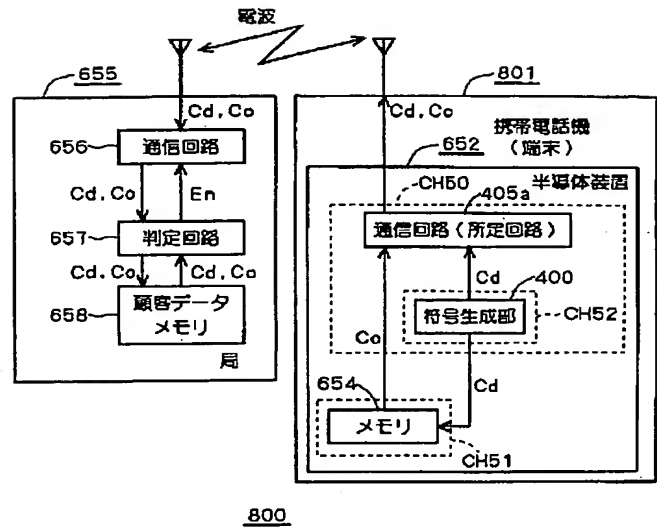
【図58】

	BL1	BL2	BL3	BL4
WL1	1	1	0	0
WL2	1	0	1	0
WL3	0	0	0	1
WL4	0	1	0	0

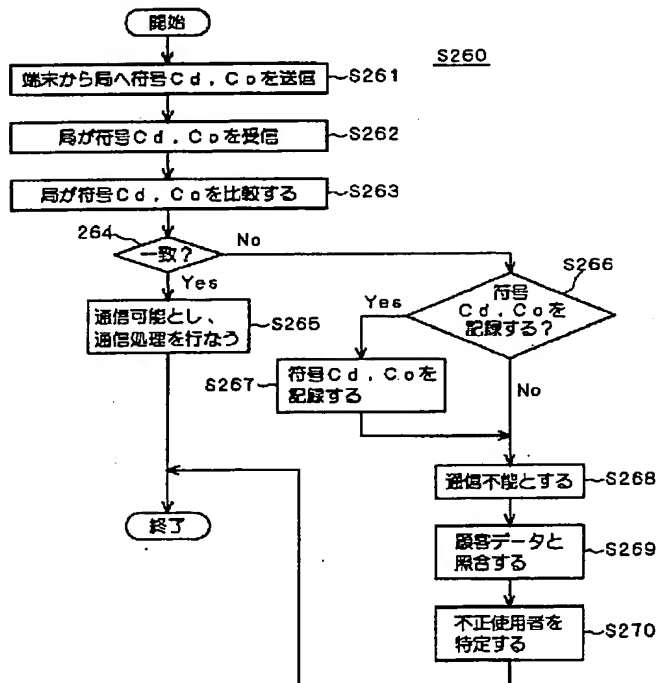
【図19】



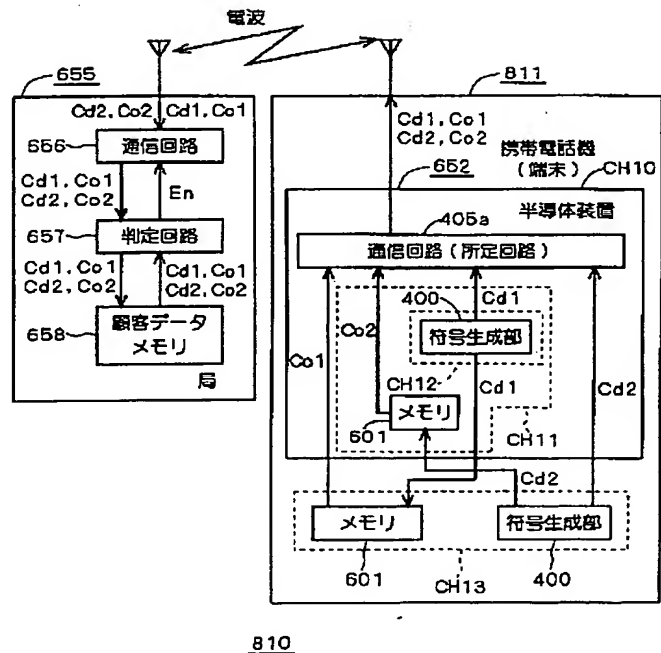
【図20】



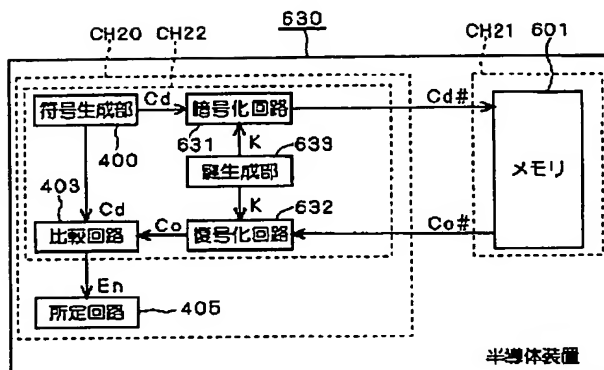
【図21】



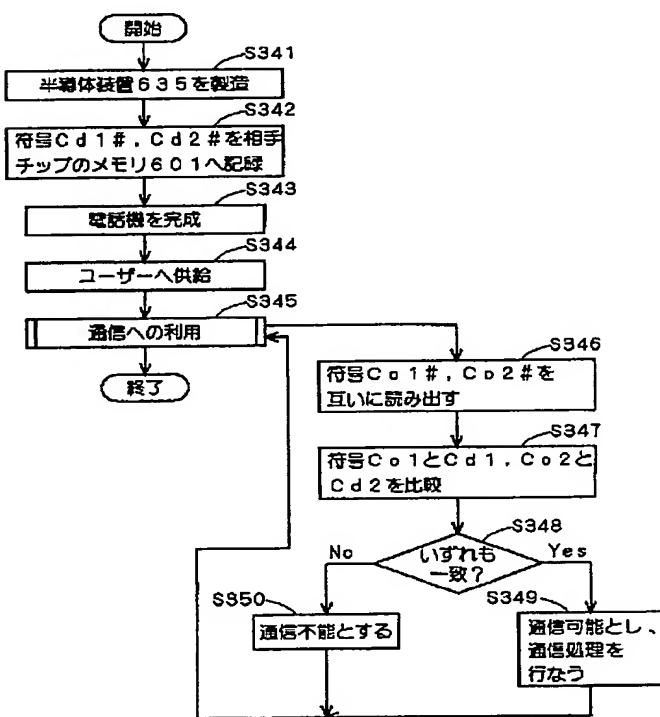
【図22】



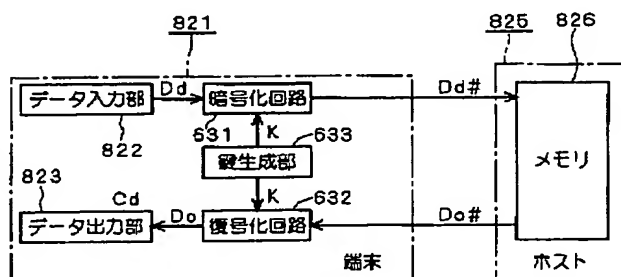
【图 2 4】



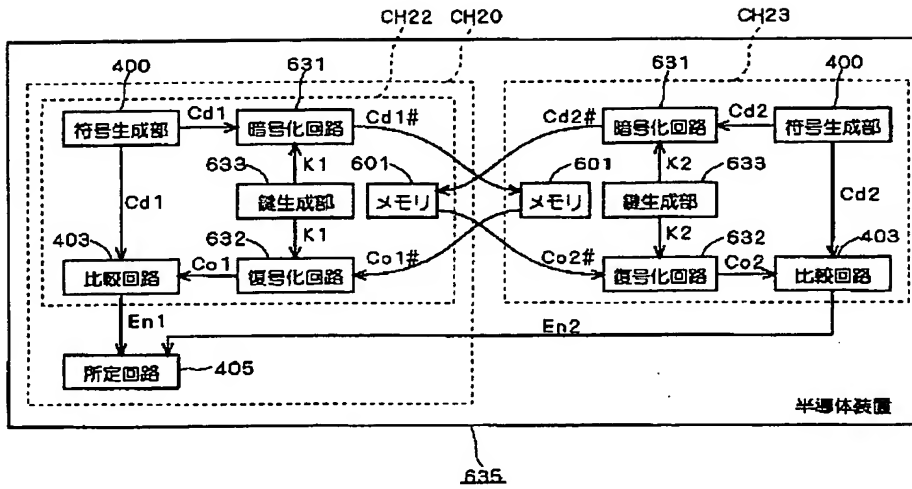
【图 29】



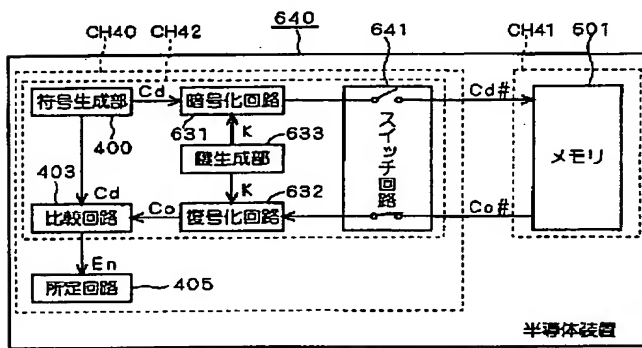
【図 3 1】



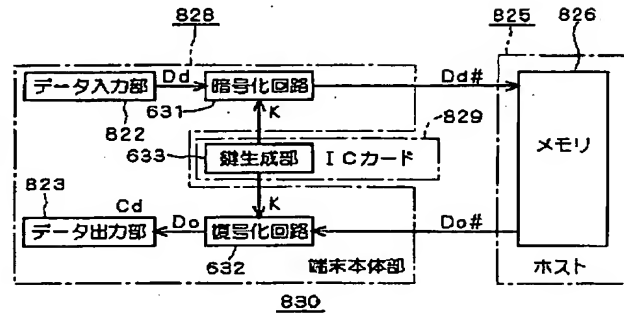
【図28】



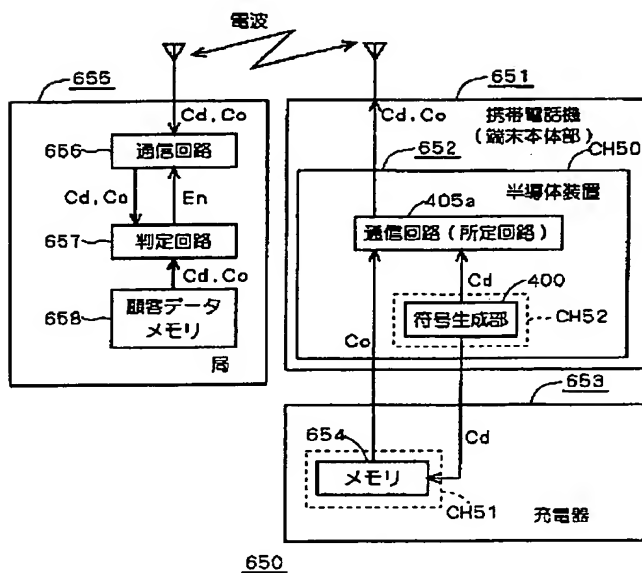
【図30】



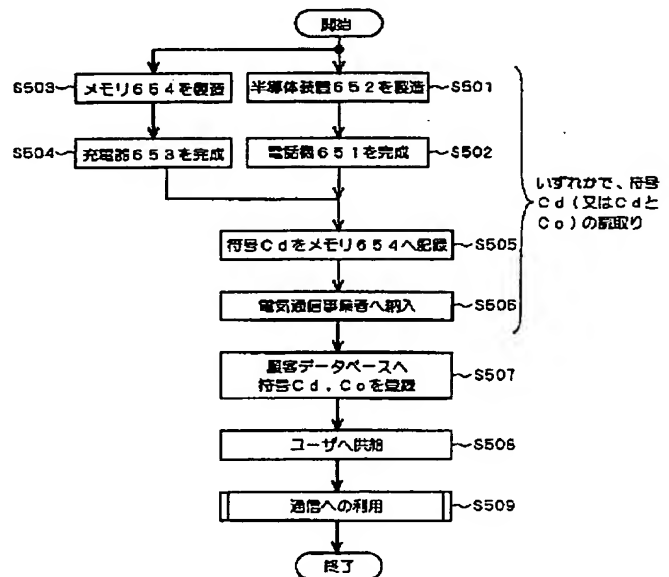
【図32】



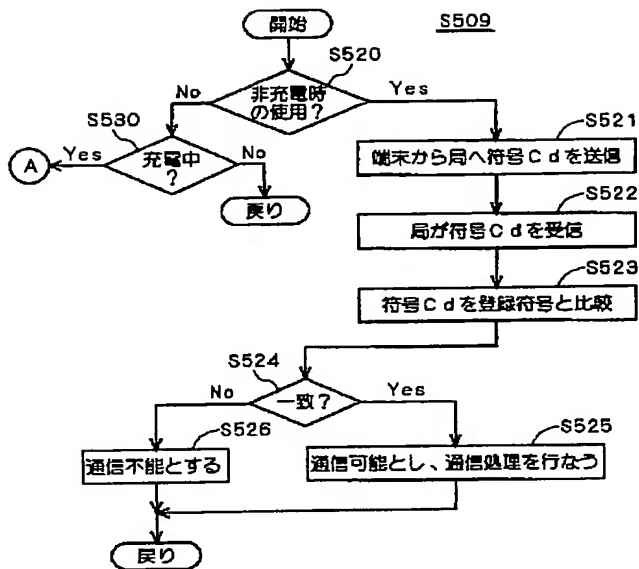
【図33】



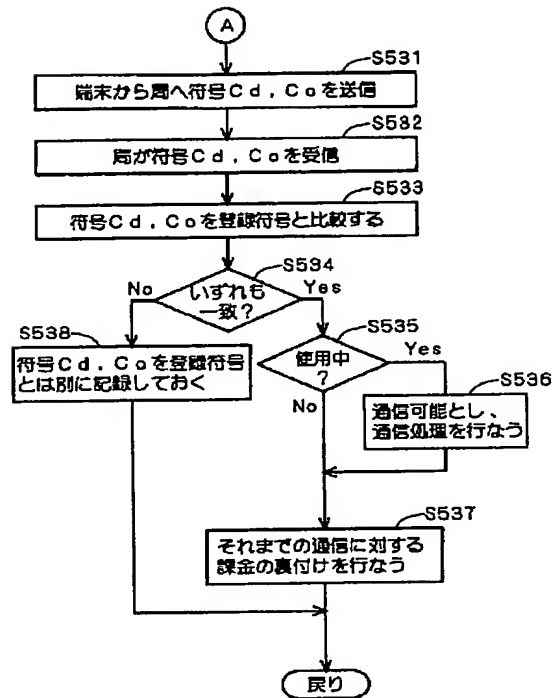
【図34】



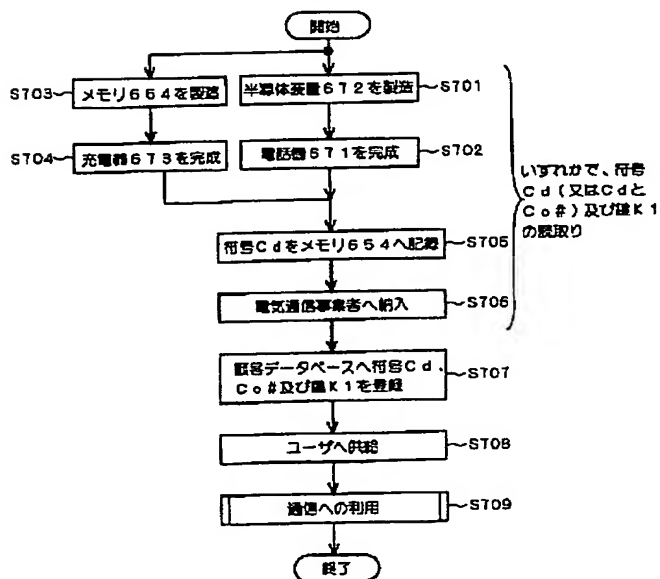
【図35】



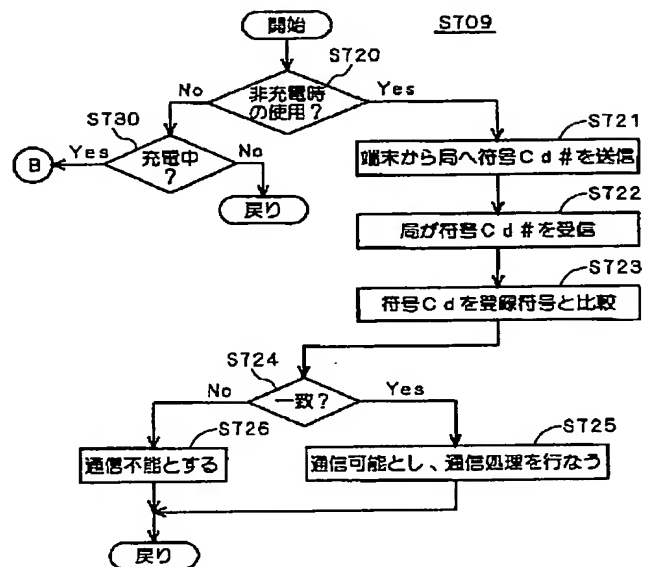
【図36】



【図38】

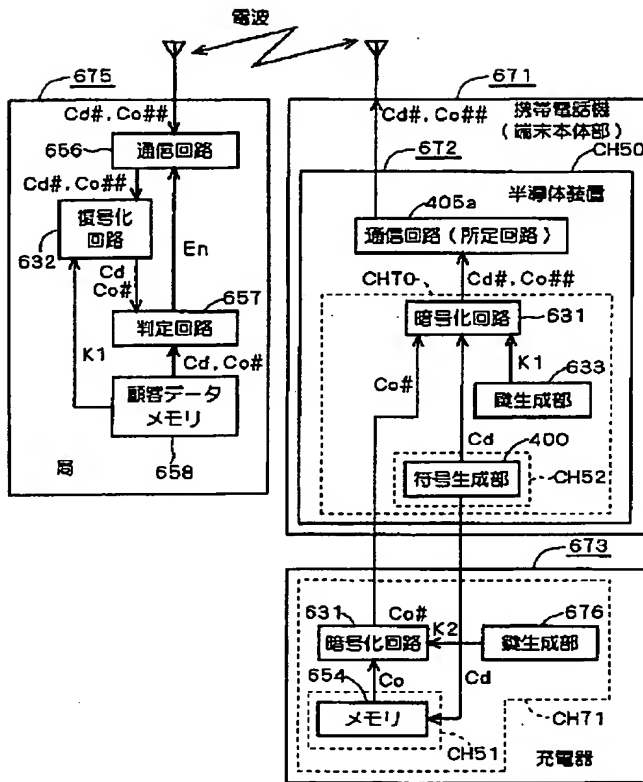


【図39】





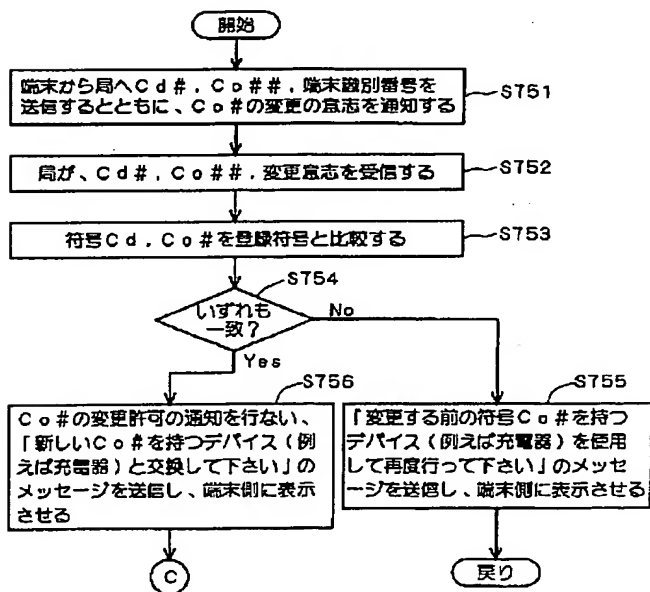
【図37】



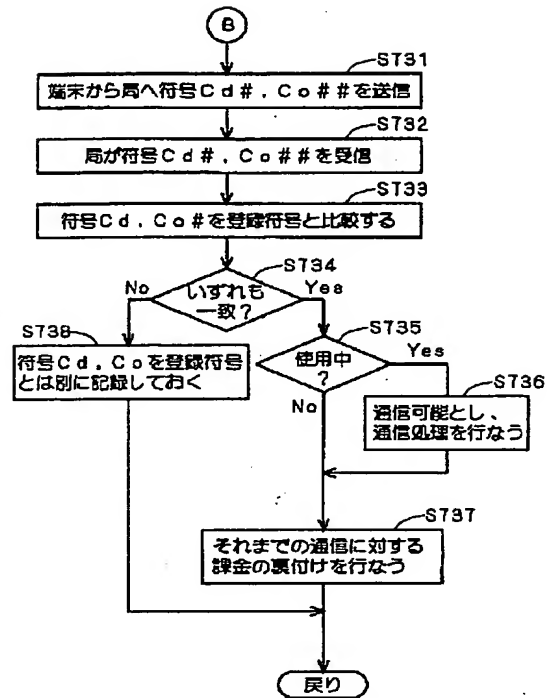
670

【図42】

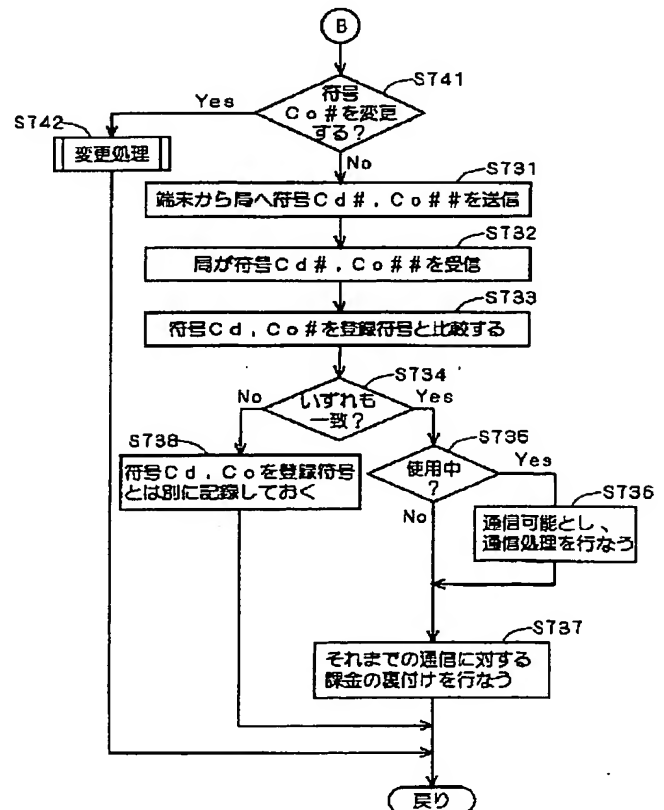
S742



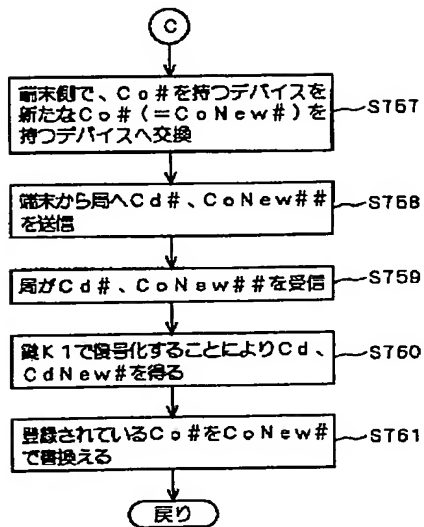
【図40】



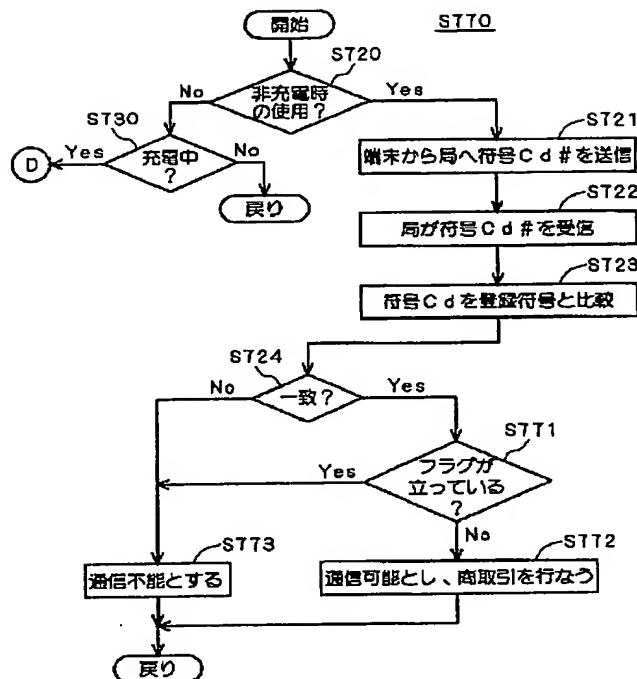
【図41】



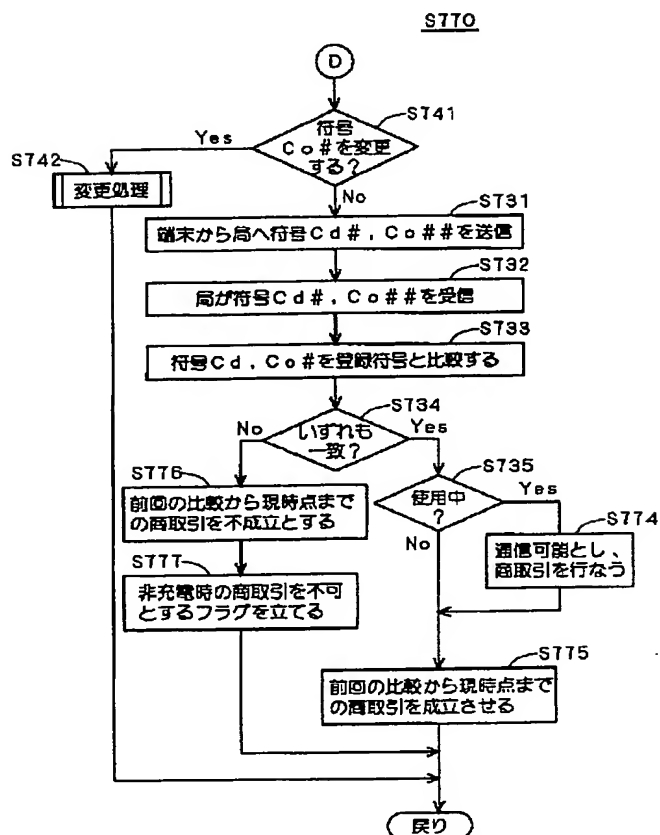
【図43】



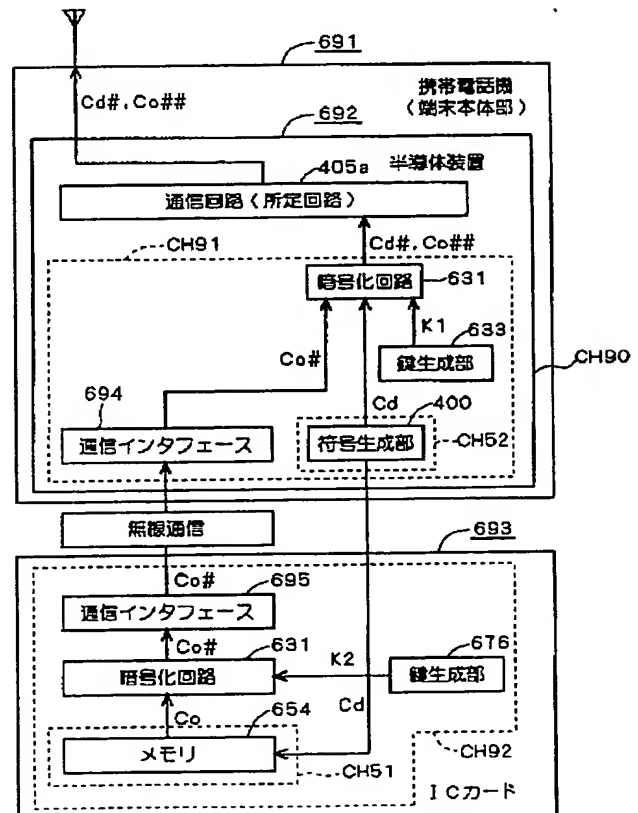
【図44】



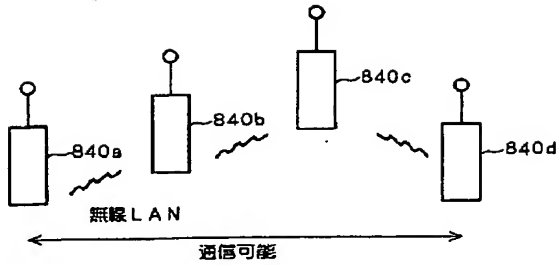
【図45】



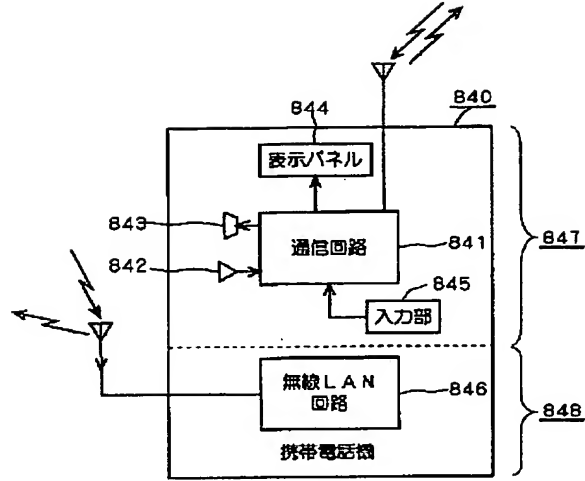
【図46】



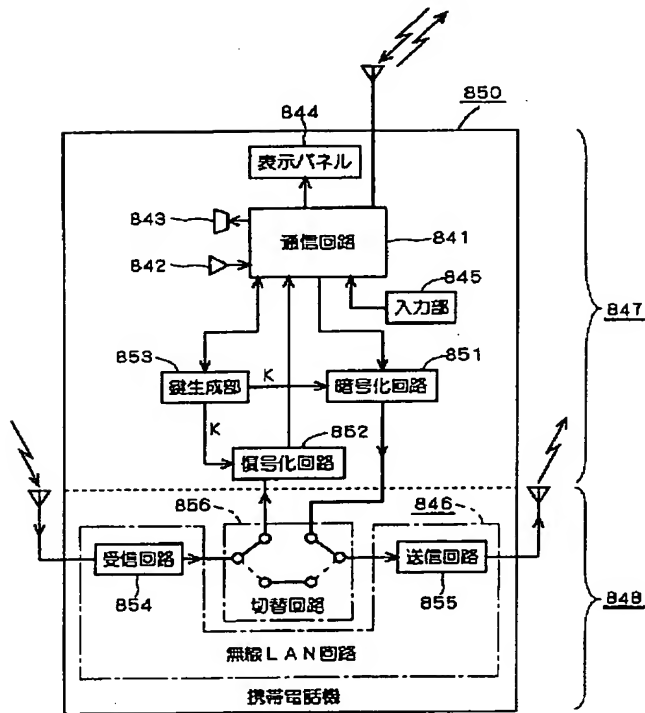
【図47】



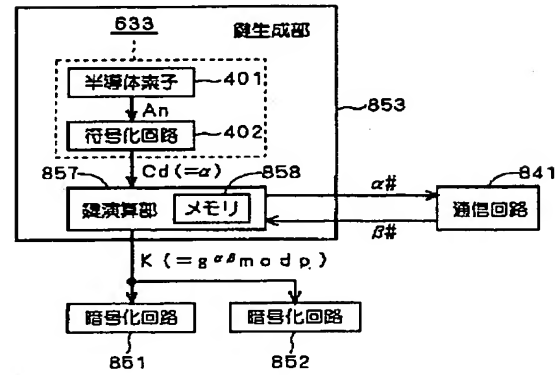
【図48】



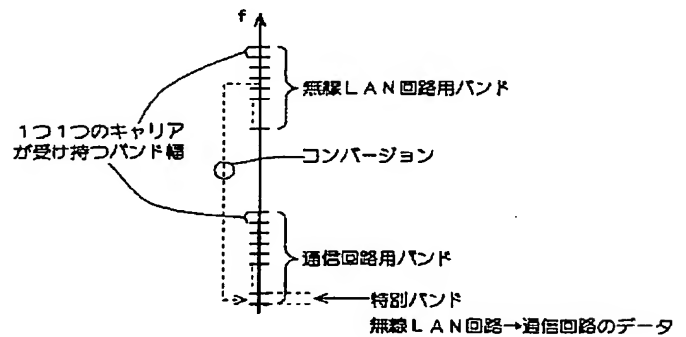
【図49】



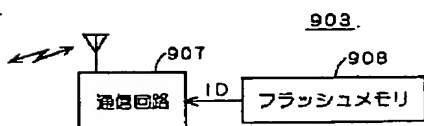
【図50】



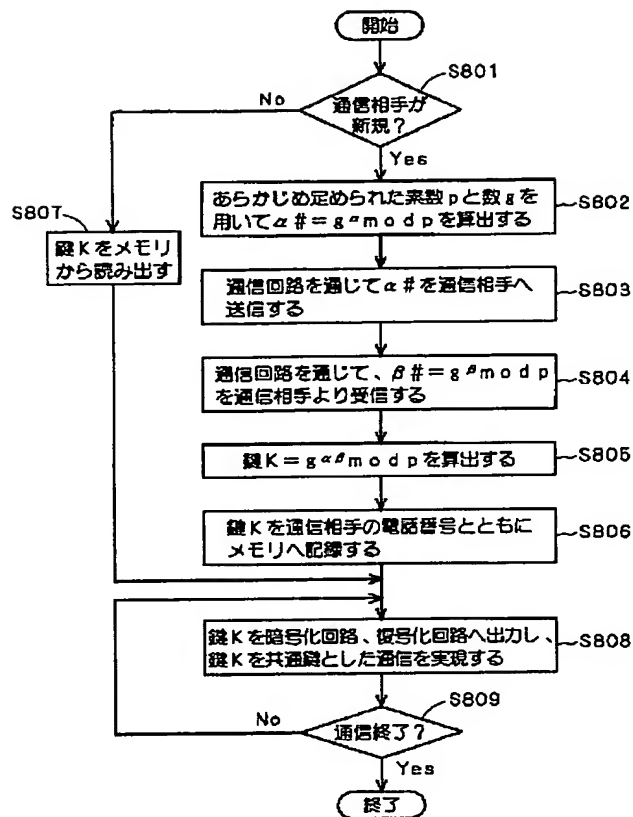
【図53】



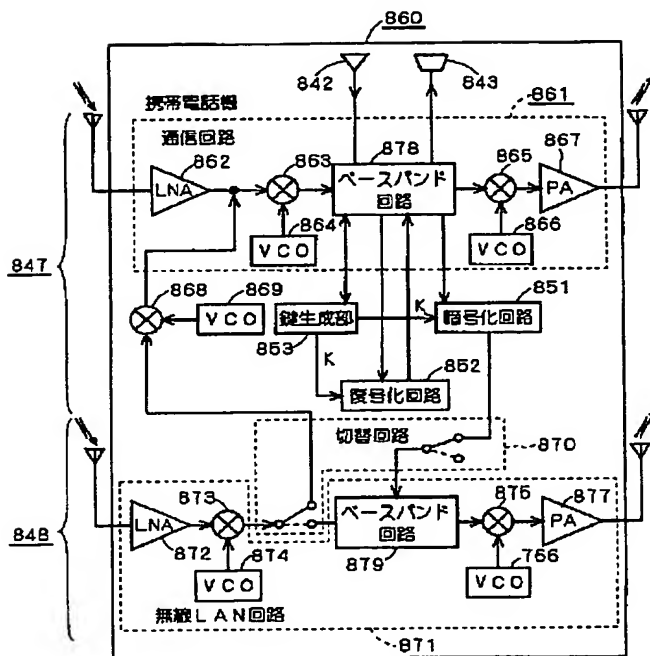
【図65】



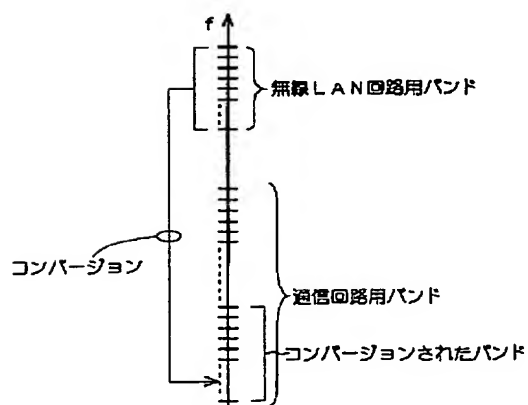
【図51】



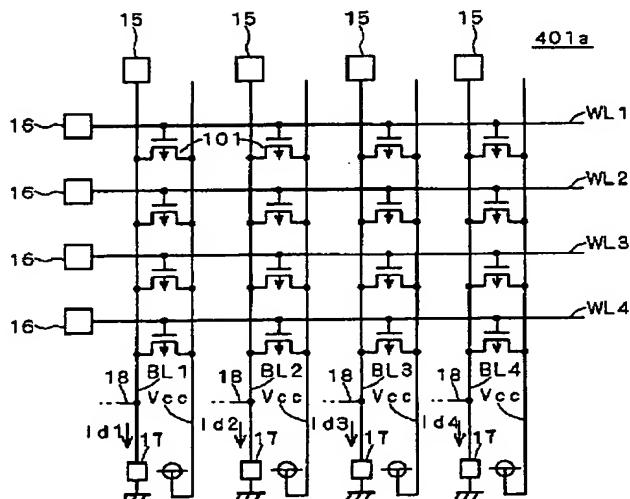
【図52】



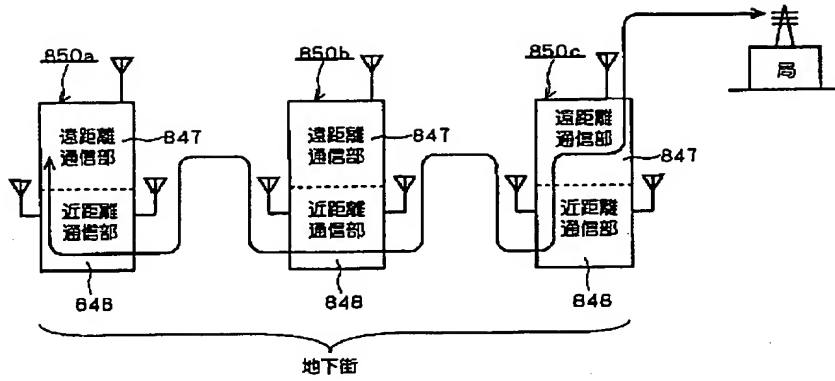
【図54】



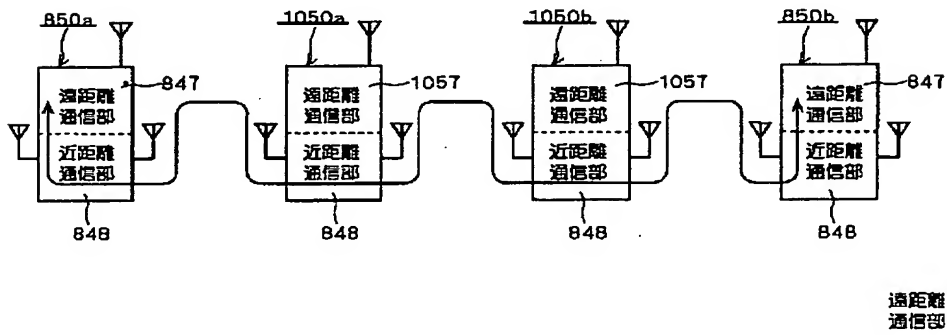
【図57】



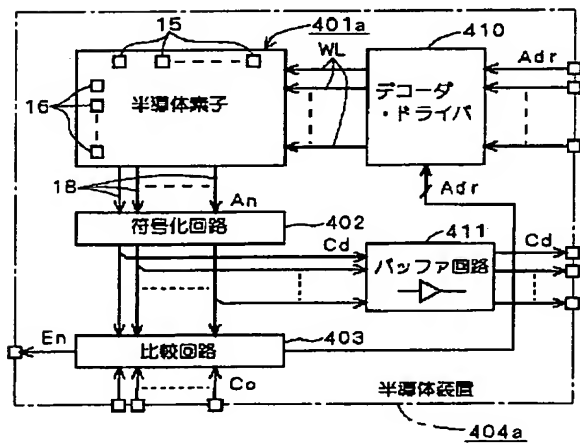
【図55】



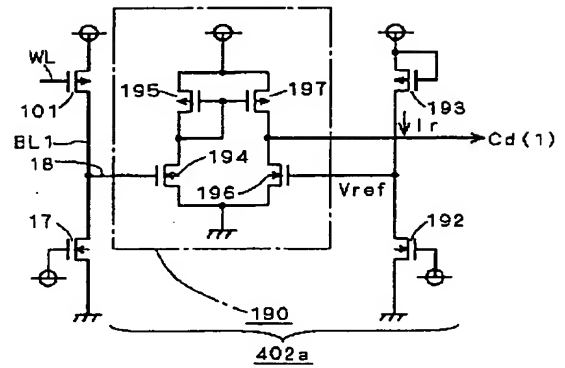
【図56】



【図59】

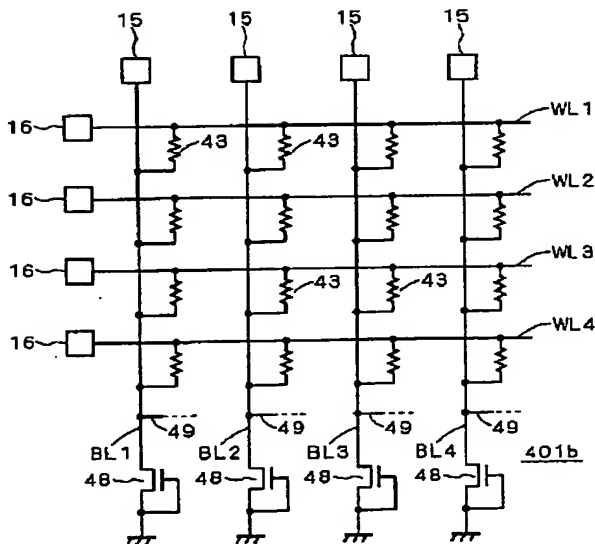


【図60】

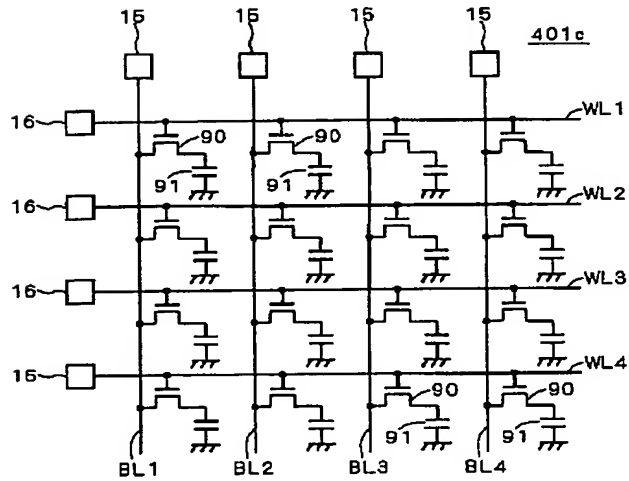




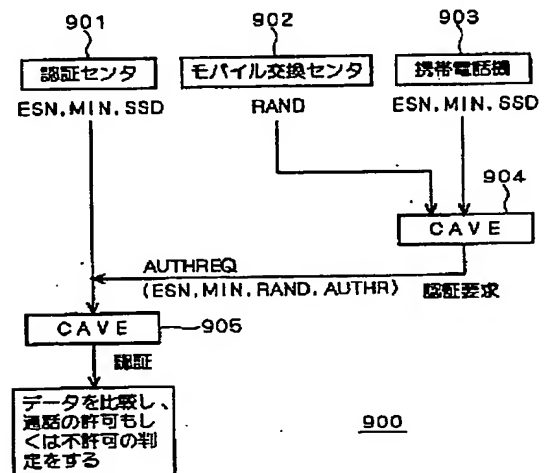
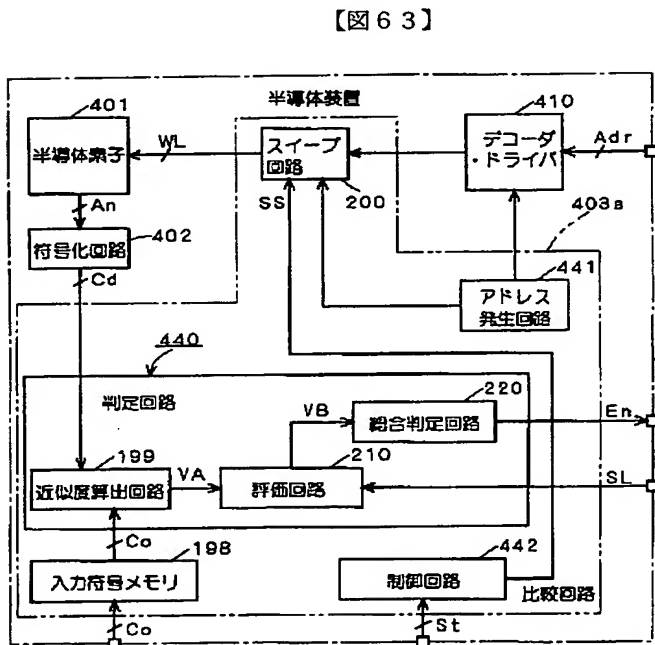
【図61】



【図62】



【図64】



フロントページの続き

(51) Int. Cl.<sup>7</sup>

識別記号

F I  
H 0 4 L 9/00

テーマコード(参考)

6 7 3 C

F ターム(参考) 5B017 AA07 BA07 BB03 CA11  
5B035 AA13 BB09 BC00 CA38  
5B058 CA27 KA02 KA04 KA08 KA33  
KA35 YA20  
5J104 AA07 KA02 NA02 NA05 NA35  
PA02  
5K067 AA32 BB04 EE02 EE10 EE16  
GG01 GG11 HH05 HH17 HH22  
HH23 HH24 HH36

**THIS PAGE BLANK (USPTO)**